2011 年度
自動車の情報セキュリティ動向に関する調査

ネットワーク化・オープン化の進む自動車にセキュリティを

2012 年 5 月

独立行政法人
情報処理推進機構
技術本部　セキュリティセンター

目次

目次 II
図目次 III
表目次 III
略語 IV
1 はじめに 1
1.1 2010 年度までの成果 1
1.2 2011 年度版の概要 2
2 国内外の自動車情報セキュリティの動向 4
2.1 欧州の自動車情報セキュリティの動向 4
2.2 米国の自動車情報セキュリティの動向 11
2.3 日本国内の自動車情報セキュリティの動向 15
2.4 自動車情報セキュリティ動向調査のまとめ 17
3 自動車情報セキュリティの脅威の動向 18
3.1 自動車情報セキュリティの脅威の事例 18
3.2 自動車情報セキュリティの脅威の事例の分析 28
4 自動車におけるネットワーク接続の動向 30
4.1 自動車のネットワーク接続の特定方法 30
4.2 車載制御システムを支える車載 LAN 31
4.3 自動車のネットワーク接続の動向分析 44
5 まとめ 47
5.1 進化する自動車と増大する脅威 47
5.2 自動車情報セキュリティの課題 48
6 自動車情報セキュリティへの提言 50
6.1 ユーザへの適切な情報提供 50
6.2 悪意ある攻撃への備え 52
6.3 今すぐ始めるセキュリティ対策 53

図目次

図 1-1 車載 LAN のアーキテクチャ(2010 年) 1
図 2-1 EVITA HSM のアーキテクチャの概要 5
図 2-2 AUTOSAR CSM と PKI 機能のインタフェース 7
図 2-3 PRESERVE プロジェクトの概要 8
図 2-4 セキュリティを考慮したプローブ情報活用モデル 16
図 3-1 自動車の外部から車載 LAN への不正侵入 18
図 3-2 パトロールカーのビデオレコーダの映像記録が漏洩する問題 21
図 3-3 RF ジャマーによる自動車の盗難 22
図 3-4 偽の GPS 信号により位置をだまされる問題 24
図 3-5 GSM 端末が偽の基地局に盗聴される問題 26
図 4-1 自動車のネットワーク接続手法の概要 30
図 4-2 ネットワーク接続手法を整理するための抽象化した車載 LAN の構造 31
図 4-3 車載 LAN の重要度別機能分類の例 32
図 4-4 CHAdeMO インタフェース仕様と接続例 35
図 4-5 ルームミラー一体型のテレマティクスモジュール- OnStar FMV 本体とリモコン 39
図 4-6 OnStar 用テレマティクス車載機の接続構成 40
図 4-7 車載 Ethernet の主な関連団体と関係 42
図 4-8 ネットワーク接続、オープン化、安全快適機能 44
図 5-1 自動車に対する脅威 47
図 5-2 自動車の情報セキュリティへの脅威 48
図 6-1 自動車情報セキュリティへの提言 50
図 6-2 ユーザへの適切な情報提供 51
図 6-3 悪意ある攻撃の認識 52
図 6-4 今すぐはじめるセキュリティ対策 53

表目次

表 1-1 略語一覧表 iv
表 4-1 機能分類の概要 33

略語

本書では以下の略語を使用する。一部は社団法人自動車技術会・基準キーワード[1]を参照している。

表 1-1 略語一覧表

略語	名称
AES	Advanced Encryption Standard
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
ATOMS	Advanced Telematics Operating System
A/V	Audio Visual
BEM	Body Electronic Module
CAN	Controller Area Network [1]
CD	Compact Disc
CHAdeMO	CHArge de Move: チャデモ協議会
CSC	Chassis and Safety Control
CSM	Crypt Service Manager
CU	Communication Unit
DoIP	Diagnostic over IP (TCP/IP)
DSRC	Dedicated Short Range Communication
DTC	Diagnostic Trouble Code
ECU	Electronic Control Unit [1]
EmSys WG	Embedded Systems Work Group
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Electric Vehicle[1]
EVITA	E-safety Vehicle Intrusion proTected Applications
FMV	For My Vehicle
FOT	Field Operational Tests
FP7	Seventh Framework Programme
FTP	File Transfer Protocol
FHWA	Federal Highway Administration

[1] 社団法人自動車技術会基準キーワード, https://tech.jsae.or.jp/rireki/keyword.pdf

略語	名称
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HMI	Human Machine Interface
HSM	Hardware Security Module
HU	Head Unit
IEC	International Electrotechnical Commission
IEEE	The Institute of Electrical and Electronics Engineers, Inc.
IP	Internet Protocol(IP 接続), Intellectual Property(IP)
IPA	Information-technology Promotion Agency, Japan
IPSec	Security Architecture for Internet Protocol
ISO	International Organization for Standardization
ITS	Intelligent Transport System [1]
ITU	International Telecommunication Union
JPO	ITS Joint Program Office
JSAE	Society Automotive Engineers of Japan: 自動車技術会
LAN	Local Area Network
LF	Low Frequency
LIN	Local Interconnect Network [1]
MOST	Media Oriented Systems Transport bus
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
OBD	On Board Diagnostics
OBD-II	On Board Diagnosis-II [1] [2]
OVAL	Open Vulnerability and Assessment Language
OVERSEE	Open VEhiculaR SEcurE platform
PC	Personal Computer
PHV	Plug-in Hybrid Vehicle
PKI	Public Key Infrastructure
PLC	Power Line Communication
PND	Portable Navigation Device
PRECIOSA	PRivacy Enabled Capability In co-Operative systems and Safety Applications
PRESERVE	Preparing Secure Vehicle-to-X Communication Systems

[2] 国土交通省「安全 OBD」, http://www.mlit.go.jp/kisha/kisha07/09/090914_2_.html

略語	名称
PRNG	Pseudo Random Number Generator
PTC	Power Train Control
RFI	Request For Information
RITA	The Research and Innovative Technology Administration
RTP	Real-time Transport Protocol
SAE	Society of Automotive Engineers
SCAP	Security Content Automation Protocol
SEIS	Security Embedded IP-based System
SPP	Serial Port Profile
SSID	Service Set Identifier
TCG	Trusted Computing Group
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TPMS	Tire Pressure Monitoring System
UAV	Unmanned Air Vehicles
UDS	Universal Diagnostic System
USB	Universal Serial Bus
USDOT	United States Department of Transportation
UTP	Unshielded Twisted Pair
V2G	Vehicle to Grid [1]
VANET	Vehicle Ad-hoc Networks
WAVE	Wireless Access in Vehicular Environments
WG	Working Group

1　はじめに

1.1　2010 年度までの成果

独立行政法人 情報処理推進機構(以下、IPA)では 2006 年度から組込みシステムの情報セキュリティの調査の一環として、自動車に関する機器の情報セキュリティ動向の調査[3]を実施してきた。2010 年度、「国内外の自動車の情報セキュリティ動向と意識向上策に関する調査[4]」を実施し、その中で以下の項目について調査を行った。

(1)　車載情報システムのセキュリティ対策の現状

(2)　普及の進む電気自動車(以下 EV: Electric Vehicle)に関する脅威と対策に関する調査

(3)　関連団体の情報セキュリティ関連動向

この結果、2010 年度は自動車の車載情報システムやタイヤの空気圧監視システムに対する攻撃手法が論文として報告されていたことがわかった。また、自動車のテレマティクスサーバを不正に使用して数十台の自動車を一斉に停止させる事件も発生しており、車載情報システムへの攻撃の動機が具体的に存在していることが明らかになった。

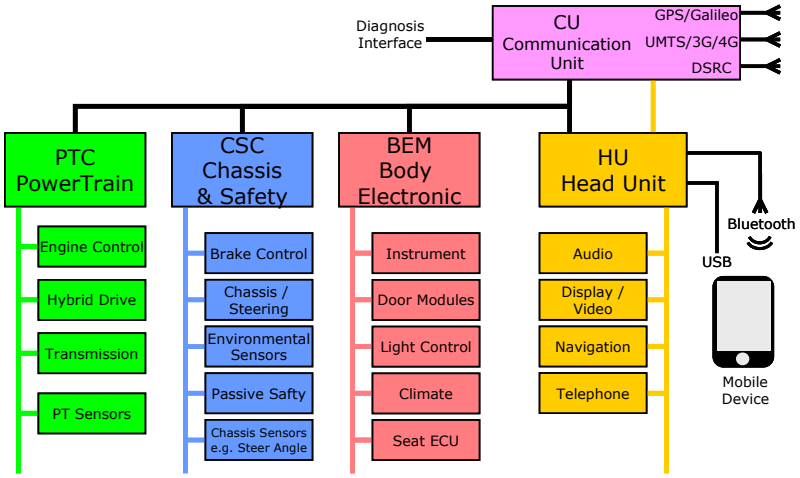

図 1-1 車載 LAN のアーキテクチャ(2010 年)

一方、車載 LAN (Local Area Network)のアーキテクチャでは、自動車の外部との接続がさらに多様になり、機能も急速に増加していく傾向が明らかになった。図 1-1 は 2010 年度版で掲載した、EVITA (E-safety Vehicle Intrusion proTected Applications)プロジェクト(以下、EVITA)から引用した車載 LAN のアーキテクチャである。この図では車載 LAN

[3] “脆弱性対策”, “組込みシステム・制御システムのセキュリティ対策関連”, IPA
http://www.ipa.go.jp/security/vuln/index.html#investigation

[4] “2010 年度 自動車の情報セキュリティ動向に関する調査報告書”, IPA, 2011-04-26
http://www.ipa.go.jp/about/press/20110426.html

上にどのような車載コンピュータ(ECU: Electronic Control Unit)が搭載されているか分かるが、情報セキュリティの観点における最重要機能の切り分けを検討することが課題として明らかになった。

1.2 2011 年度版の概要

1.2.1 調査の目的

今日の自動車一台に搭載される ECU は 100 個以上、ソフトウェアの量は約 1,000 万行と言われており大規模になっている[5]。自動車のコストに占めるエレクトロニクス部品の割合はエンジン車で最大 30%、ハイブリッド車では 50%、電気自動車では 70%に達する[6]。さらに、複数の車載カメラなど画像処理のために 100Mbps 以上の高速で大容量の車載ネットワークが求められている。また、自動車の外部とのインタフェースは OBD-II (On Board Diagnosis-II)と充電制御インタフェースのほかにも、スマートフォンやタブレット PC (Personal Computer)が持ち込まれるようになるなど多様化している。

本調査は、自動車の情報セキュリティ対策の普及啓発を推進するために、昨年度に引き続き自動車の情報セキュリティの動向や対策について、主にネットワーク接続手法と持ち込み機器に関して調査検討を行い、その結果を自動車に関連する開発者向けの報告書としてとりまとめることを目的とする。

1.2.2 調査の内容

今年度は、昨年度調査で明らかになった課題を踏まえた上で、自動車のネットワーク接続及び情報セキュリティに関する動向の調査、対策の検討などを行うとともに、自動車のネットワークを利用した脅威について整理した。

検討体制としては、昨年度に引き続き、自動車及び情報セキュリティに関する有識者、業界関係者からなる研究会及びディスカッショングループを設置し、検討を行った。具体的な調査項目は、以下の通りである。

(1) 自動車の情報セキュリティの動向と対策
(2) 自動車のネットワーク接続の動向
(3) 自動車の機能分類とそれに対する脅威の分析

---

[5] “【ESC 2011】IBM が語る電気自動車「シボレー・ボルト」のソフトウェア開発”, EE Times Japan, 2011-05
http://eetimes.jp/ee/articles/1105/09/news113.html

[6] “平成２１年度地域活性化推進調査「自動車の電子化に係る欧州産学官連携と地域産業振興調査」”
“第２章 自動車関連技術の最近の動向”, 中国経済産業局, 2011-04-22
http://www.chugoku.meti.go.jp/research/h21fy/jidousha.html

1.2.3 調査の結果

2011 年度の調査から、車載情報システムは急速に進化しているが、情報セキュリティ対策が伴っていない場合が見られ、時代と環境の変化に伴い、新たな情報セキュリティ対策が必要であることが明らかとなった。

2011 年度には研究事例として、車内からだけではなく、外部から携帯電話網を使って車載情報システムに侵入、攻撃する手法に関する論文が発表されている。この論文は特定の車種を対象とした実験ではあるが、攻撃者が対象の自動車のドアやボンネットには触れることなく、ドアロックを解除するなどの攻撃に成功している。他にも、偽の基地局と通信して盗聴される例、偽の GPS (Global Positioning System)衛星に誘導される例など、自動車のネットワーク接続手法そのものに脆弱性が含まれる事例が報告されている。サーバについては、国内自動車メーカのカナダ現地サイトから 28 万人分以上の顧客情報が流出する事件があり[7]、自動車ユーザへの攻撃に利用されないかが懸念される。

欧州調査では、EVITA や PRESERVE (Preparing Secure Vehicle-to-X Communication Systems)などのプロジェクトが車載用のセキュリティハードウェアの研究開発を進めており、一部は AUTOSAR にも取り入れられていることがわかった。また欧州では、車載 Ethernet と TCP/IP (Transmission Control Protocol/Internet Protocol)に関する研究開発と標準化作業が複数存在しており、2014～2018 年ごろに市販車に投入される見込みである。Ethernet 及び TCP/IP が利用されるようになると、自動車の保守・修理や検査を高速で行えるようになり、インターネット上のサービスとの連携も行いやすくなるが、既存の車載 LAN である CAN (Controller Area Network)や LIN (Local Interconnect Network)のような専用通信手順に比べて攻撃が格段に簡単になると考えられる。

米国調査で訪問した展示会「International CES 2012」[8]では、車載オーディオ機器とスマートフォンアプリを連携させる利用方法が普及し、多くの車載オーディオの展示品が対応済みであった。またテレマティクスサービスの API (Application Programming Interface)を 2012 年中ごろに公開予定としている企業もあった。米国の自動車業界ではネットワーク接続が一般的になりつつあり、アフターマーケットを含めて早急に市場に導入しなければならないという雰囲気を感じられた。

日本国内でのヒアリングでは、充電制御インタフェースの CHAdeMO (CHArge de Move)方式がアナログ方式とデジタル方式を組み合わせることで情報セキュリティへの配慮をしていることがわかった。また、電気自動車(EV)の中には EV 用の情報を安全に出力するための専用ゲートウェイ装置を販売している部品メーカもあった。

これらの調査結果を参考としつつ、自動車開発者が情報セキュリティへの取組みに着手できるよう、研究会での検討を通じて本報告書をとりまとめた。

---

[7] “ホンダ・カナダ向けサイトの顧客情報流出、集団訴訟に発展”, 日経 ITPro, 2011-06-09
http://itpro.nikkeibp.co.jp/article/COLUMN/20110607/361114/

[8] International CES, http://www.cesweb.org/

2　国内外の自動車情報セキュリティの動向

本章では、欧米及び国内における自動車情報セキュリティの動向調査の結果を報告する。

2.1　欧州の自動車情報セキュリティの動向

2010 年度の自動車情報セキュリティで行った欧州の動向調査では、EVITA において、車載 LAN 通信用のセキュリティ機能をハードウェアで実装する研究開発が行われていることがわかった。2011 年は EVITA が開発したセキュリティ仕様とハードウェアセキュリティモジュール(Hardware Security Module : 以下、HSM)のプロトタイプについて成果報告が行われるとともに、EVITA の後継にあたるプロジェクトが開始されている。ここでは EVITA 及び後継プロジェクトである PRESERVE と、欧州における自動車セキュリティの国際会議 escar 2011 についての調査結果を報告する。

2.1.1　EVITA プロジェクトの動向

EVITA は、EU (European Union)の FP7 (Seventh Framework Programme)という研究予算の支援を受け、車載 LAN のセキュリティを保護する通信手順と実行処理基盤を研究開発するプロジェクトである。プロジェクトの成果としては、リアルタイム処理に対応した暗号化処理機能などの EVITA のセキュリティ仕様を FPGA (Field-Programmable Gate Array)上にハードウェアとして実装し、所定の乱数機能、暗号化処理、メッセージ署名などのセキュリティ機能と、所定のリアルタイム処理性能が得られたと報告している。

EVITA の基本的な機能は、既存の車載 LAN 通信についてメッセージ署名や暗号化などによって保護することである。既存の車載 LAN 通信としては CAN、LIN、FlexRay、MOST (Media Oriented Systems Transport bus)などが想定されている。将来的には TCP/IP 化することで車載 LAN の通信をすべて IP 化する見通しも示されている[9]。

EVITA のセキュリティ仕様は車載システムに求められるセキュリティ性能及び機能によって light, medium, full の 3 つのレベルがある。このうち下位レベルの light と medium という仕様にほぼ相当する製品を Infineon 社が製造・販売している。EVITA の上位レベルにあたる full というタイプの市販品はまだなく、EVITA などの後継プロジェクトである「PRESERVE プロジェクト」において、他の車載ソフトウェアのセキュア実装技術と統合した ASIC (Application Specific Integrated Circuit)としてハードウェア化され、車載の実証実験が行われる予定である。PRESERVE プロジェクトについては2.1.2 で紹介する。

---

[9] “EVITA Deliverable 2.1: Specification and evaluation of e-security relevant use cases”
“2.2.6 New approaches towards IP-based in-car network architecture”, 2009-12
http://evita-project.org/Deliverables/EVITAD2.1.pdf（無料登録で閲覧可能）

2.1.1.1　EVITA ハードウェアセキュリティモジュール(HSM)の概要

図 2-1 は EVITA D3.2 で示されている EVITA HSM のアーキテクチャの概要である。

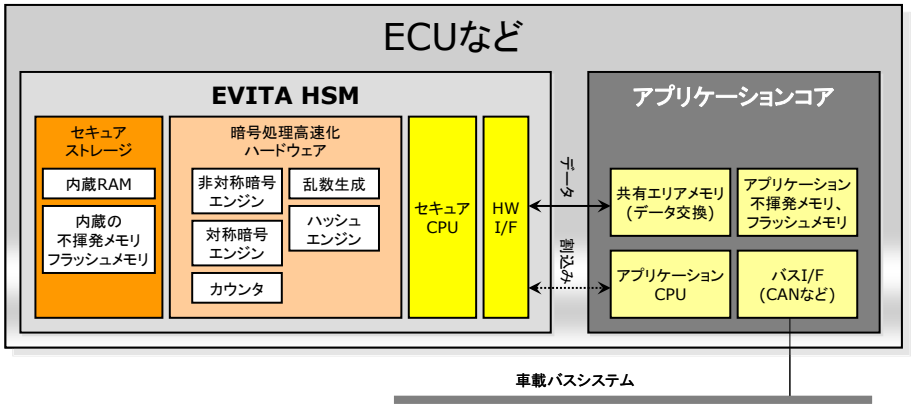

図 2-1 EVITA HSM のアーキテクチャの概要

EVITA では ECU や主要なアクチュエータやセンサに EVITA HSM を搭載することを想定しているため、図の右にある特定のアプリケーションを実行するための「アプリケーションコア」と、図の左側の「EVITA HSM」からなっている。車載バスシステムとの通信機能はアプリケーションコア側にあり、CAN や LIN、FlexRay など個別の車載バスに応じて通信を行う。

例えばブレーキ制御を行う機能が搭載された ECU の場合、アプリケーションとしてブレーキを制御するソフトウェアが実行され、他の ECU と通信する際に EVITA HSM を使って、他の ECU との通信内容を保護する。EVITA HSM の特徴としては、このような処理がリアルタイムに複数セッションで並列に可能な点である。

図 2-1 にある EVITA HSM の機能のうち、「非対称暗号エンジン」は公開鍵暗号などの暗号化処理を、「対称暗号エンジン」は AES (Advanced Encryption Standard)や楕円暗号処理などの暗号化処理を行う。「ハッシュエンジン」はメッセージ署名などのためのハッシュ関数の処理を行う。「カウンタ」は暗号化されたメッセージやブロックの順番や番号を特定し、暗号化ハードウェアが暗号化処理に利用する。「乱数生成」は対称暗号化のための新しい鍵の生成や、予測されにくい初期値の生成などに利用する。乱数の生成は出力される値の偏りがないことが求められるが、EVITA HSM の場合は軽量な実装の EVITA light に擬似乱数生成機能である PRNG (Pseudo Random Number Generator)を、中機能以上の medium, full にハードウェアによる乱数生成機能である TRNG (True Random Number Generator)を搭載する仕様である。

2.1.1.2 EVITA HSM の利用方法

EVITA HSM を自動車の ECU 製品で利用する場合は、EVITA HSM を搭載したマイコン製品を ECU などに組み込む必要がある。

ソフトウェア開発で EVITA を利用する場合、既存の車載 LAN プロトコルのメッセージを暗号化したり、メッセージ署名を付加するなどの処理を追加開発する必要がある。現時点では CAN や LIN などの車載 LAN プロトコルに関して標準的な暗号化やメッセージ署名を付加する標準は見当たらないため、独自に開発するか、EVITA に対応したセキュリティフレームワークである EMVY を利用してソフトウェアを開発する必要がある。

2.1.1.3 AUTOSAR における HSM の適用例

AUTOSAR は車載の情報システムについて、基本的な機能をソフトウェア部品として共通化し、さまざまな ECU 上の実行環境で実行可能にする標準化を行っている。EVITA では AUTOSAR 環境を利用して検証用の実装を行うにとどめ[10]、直接的に AUTOSAR への標準化提案は行っていないが、EVITA のセキュリティ仕様の一部に当たる機能は AUTOSAR でもインタフェースが標準化されている。

AUTOSAR では個別の機能は"Service Manager"シリーズとして個別に標準化されている。このうち AUTOSAR リリース 4 で暗号化処理などを行う CSM (Crypt Service Manager) が新たに標準化された[11]。

---

[10] "Deliverable D1.2.5.2:Presentation Slides from the Final EVITA Workshop on Security of Automotive On-Board Networks", EVITA Project, 2011-11-23

[11] "AUTOSAR architecture expands safety and security applications", AUTOSAR, Stefan Bunzel, 2011-02-17
http://www.eetimes.com/design/automotive-design/4213069/AUTOSAR-architecture-expands-safety-and-security-applications
"Requirements on Crypto Service Manager", AUTOSAR, R4.0 Rev 1, 2009-11-30
http://www.autosar.org/download/R4.0/AUTOSAR_SRS_CryptoServiceManager.pdf

以下の図2-2は自動車向けの組込みセキュリティのカンファレンスである"escar 2011[12]"で、Bosch 社が AUTOSAR 環境での暗号化機能の API について発表した資料の一部である。Bosch 社は自動車用 ECU や部品を開発・販売する世界的な企業であり、EVITA プロジェクトに正式メンバーとして参加している。また、AUTOSAR では標準化の方針を決定する 9 社のコアメンバーのうちの 1 社である。

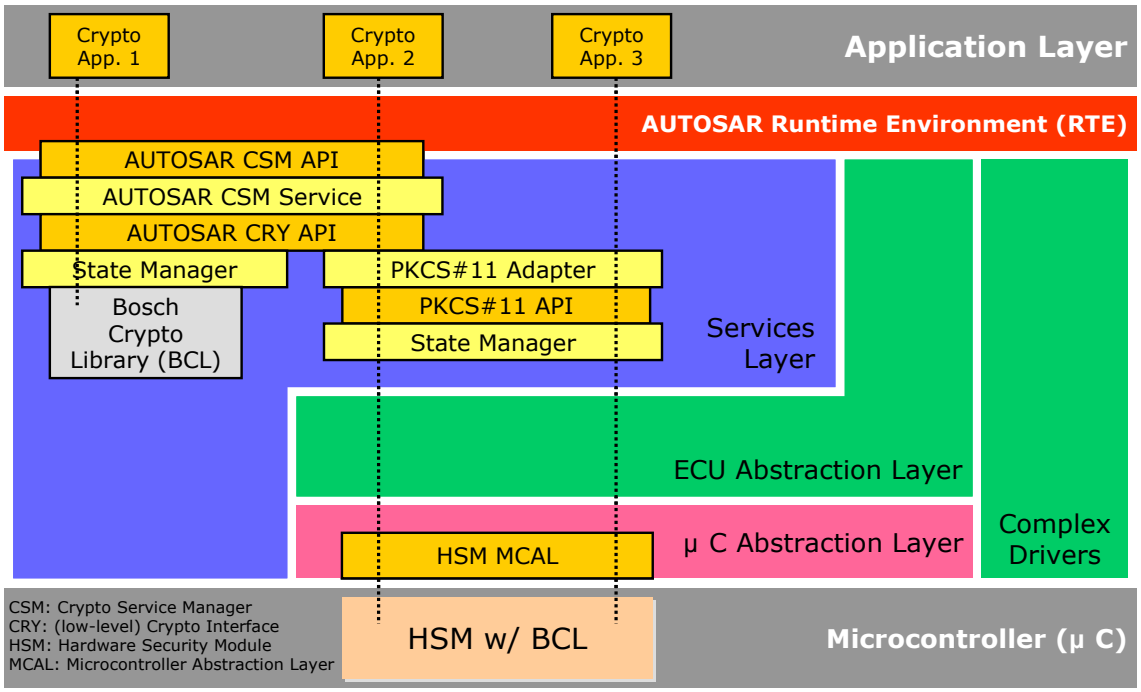

図 2-2 AUTOSAR CSM と PKI 機能のインタフェース

図の上にある「Crypto App」は暗号化機能を利用するアプリケーションである。AUTOSAR のアプリケーションは RTE (Runtime Environment) と呼ばれる共通の実行環境で実行され、RTE 上で API を呼び出す。ここでは AUTOSAR 環境で暗号化機能を利用する 3 つのパターンについて説明している。Crypto App 1 と Crypto App 2 は AUTOSAR 標準の CSM API を利用して暗号化機能を利用している。CSM の内部では Bosch 社の Bosch Crypto Library が暗号化機能をソフトウェア処理で実現している。

AUTOSAR 環境で HSM を利用する場合は、Crypto App. 2 から CSM を経由して PKCS#11 Adapter を利用する方法と、Cyrpto App. 3 のように直接 PKCS#11 Adapter を呼び出す方法が提供されている。PKCS#11 はハードウェアセキュリティモジュールを利用して鍵処理や暗号化処理を実行させるための標準的な API で、公開鍵や電子証明書の媒体処理なども含まれるため機能が多い。Bosch 社では、AUTOSAR の CSM の API だけでは機能が不足した場合に HSM を直接呼び出せるとしている。

---

12 "9th escar Embedded Security in Cars Conference",
"A Hardware Security Module for Engine Control Units", isits, 2011-11-10

2.1.2 EVITA 後継プロジェクト「PRESERVE」

2.1.2.1 PRESERVE の概要

PRESERVE (Preparing Secure Vehicle-to-X Communication Systems)プロジェクト[13](以下、PRESERVE)はこれまでの SeVeCom 以降の車車間、路車間通信(V2X[14])機能と、関連する情報セキュリティ機能を統合して市場に送り出すためのプロジェクトである。プロジェクトの総予算は約 540 万ユーロで、EU FP7 フレームワークの研究開発支援を約 380 万ユーロ受けている。期間は 2011 年 1 月から 4 年間、2014 年末までとなっている。2012 年 3 月現在、PRESERVE の Web サイト [13] には、ドキュメントのレビュー中とあり、成果物(Deliverable)はまだない。PRESERVE の説明資料としては、EVITA の終了ワークショップイベント[15]で発表された資料[16]がある。

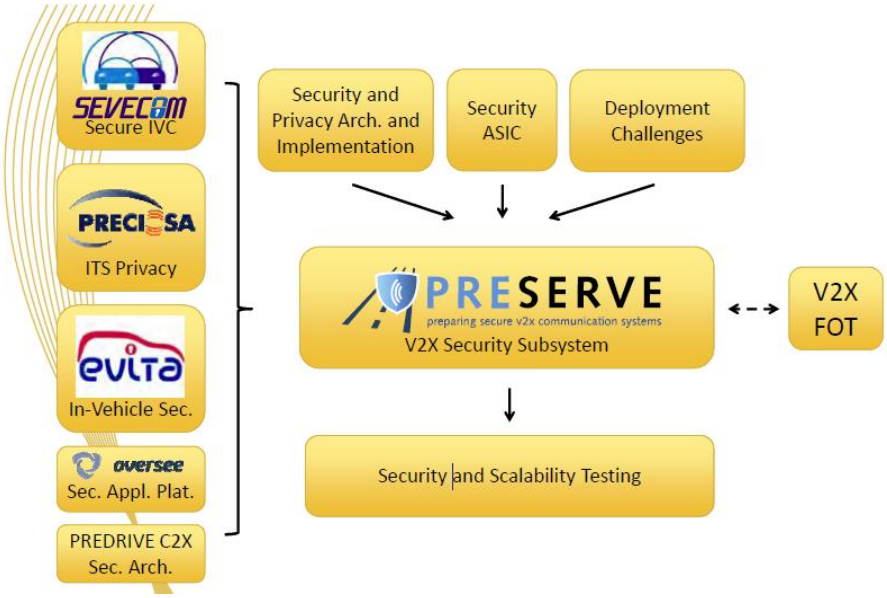

図 2-3 PRESERVE プロジェクトの概要

図 2-3 は EVITA の終了ワークショップイベントで発表された資料 [16] から引用した PRESERVE プロジェクトの概要である。PRESERVE に統合される自動車の情報セキュリティ機能として、PRECIOSA (PRivacy Enabled Capability In co-Operative systems and Safety Applications)プロジェクト[17]のプライバシ機能、EVITA プロジェクトの車載情報シ

[13] PRESERVE プロジェクト, http://www.preserve-project.eu/
[14] V2X : Vehicle to X の略で、自動車と自動車同士の間である車車間と、自動車と地上の路側機、自動車と家、自動車とスマートグリッド(V2G)など、自動車とインフラ一般との間の通信を含む。
[15] "Final EVITA Workshop", EVITA, Car2Car Forum, 2011-11-23
http://ec.europa.eu/information_society/activities/esafety/doc/2011/evita_workshop_progr.pdf
[16] "EVITA & PRESERVE, Uptake of EVITA in PRESERVE", Frank Kargl, TWENTE 大学, 2011-11-23
http://evita-project.org/Publications/EVITAD1.2.5.2.pdf
[17] PRECIOSA プロジェクト, http://www.preciosa-project.org/

ステムの保護機能、OVERSEE (Open VEhiculaR SEcurE platform)プロジェクト[18]の仮想マシン上でのアプリケーション実行基盤機能がある。V2X 全体に共通する基本的な情報セキュリティについては SeVeCom[19]から引き継がれている。

PRESERVE ではこれらの機能を統合した上で、市場規模で導入可能なことを検証する。そのため統合した機能を ASIC としてハードウェア実装を行い、市場に投入可能な価格で実現することを目的としている。さらに市場規模で普及できることを検証するため、数百台程度の実車に装着してフィールド試験(FOT: Field Operational Test)を行う予定である。2012 年にウィーンで開催される ITS 国際会議(ITS: Intelligent Transport System, ITS World Congress)では PRESERVE のデモを予定している。

2.1.2.2 PRESERVE の実証試験計画

PRESERVE では ASIC によるセキュリティ仕様の設計とハードウェアへの実装作業を計画している。ASIC による実装の価格は 1 個 100 ユーロ程度のコストで、500 個ほど製作する予定である。EVITA で開発した FPGA は 1 個 4,000 ユーロ程度だったことに比べると、実証実験用としても十分に低価格化されている。最終的に市場に投入する際は ASIC 1 個あたり 10 ユーロ程度を見込んでいる。

PRESERVE で開発する ASIC に搭載する EVITA の機能は、まだ市場に製品がない最上位の EVITA full であり、車載 LAN のゲートウェイとして 1 台の自動車に 1 個だけ搭載、する形で試験を行う。そのため EVITA medium や light の軽量な機能が、いくつかの ECU やセンサなどに複数個搭載される形にはなっていない。

PRESERVE が予定している成果には、ASIC 実装以外に、電子証明書などを扱うバックエンド機能もある。EVITA full では非対称暗号も利用でき、楕円曲線暗号を使った ECDSA、ECDH を搭載している。このため電子証明書を発行、検証、失効させるなどの機能についても、開発成果のひとつとして挙げられており、規模的な動作についても検証する計画である。

電子証明書については組込み機器用に標準化された電子証明書の標準 IEEE 1609.2[20]に対応した、証明書管理を行うバックエンド機能を開発する予定である。PRESERVE で応用する電子証明書は特に、複数の電子証明書の利用、10 年前後の長期間の証明書の識別、特殊な通信でのプライバシ保護などの応用が想定されている。

これらの開発成果を基に、2012 年から 10〜30 台のフィールド試験を実施し、その後、100 台程度の試験をフランスと米国で計画している。米国での試験は 2013 年以降に行う見込みである。

---

[18] OVERSEE プロジェクト, https://www.oversee-project.com/

[19] “Project Documents”, SeVeCom, 2008-02, http://www.sevecom.org/Pages/ProjectDocuments.html

[20] “IEEE 1609, 3rd ETSI TC--ITS Workshop ETSI TC ITS Workshop”, ETSI, 2011-02-09 http://docbox.etsi.org/workshop/2011/201102_ITSWORKSHOP/08_INTERNATIONAL_ITS_STANDARDIZATION/IEEE_KURIHARA.pdf

2.1.3　自動車組込みセキュリティ会議「escar 2011」

「escar (Embedded Security in Cars)」は毎年ドイツで開催されている、自動車向けの組込みセキュリティに関連した発表を行う会議である。2011 年は 9 回目の開催で会期は 2 日間、参加者は約 80 名であった。前回よりもドイツ以外からの参加者が若干増え、ドイツ国内から約半分、その他は米国、日本、英仏、韓国などからの参加があった。

主催はドイツで情報セキュリティ教育を提供する isits 社で、共同して運営にあたっているのが、組込みセキュリティ向けにソフトウェア製品の受託開発を行う escrypt 社である。参加者のうち大学・研究機関は 1 割程度で、ほとんどの参加者が自動車業界と半導体業界である。

2.1.3.1　「escar2011」へ参加した情報セキュリティ関連企業・組織

escar 2011 ではスポンサーとして McAfee 社と TCG (Trusted Computing Group)が参加・出展していた。

McAfee 社はパソコン向けのウイルス対策ソフト製品の主なメーカのひとつであり、Intel による買収後、組込み向けのセキュリティ製品をリリースしている。escar 2011 では展示用のボードとともにセキュリティ製品を展示していた。

TCG (Trusted Computing Group)[21]は、情報通信機器向けにソフトやデータの検証・証明機能を提供する TPM などの標準化と普及を行う業界団体である。TCG では 2011 年から組込み向けのワーキンググループとして「EmSys WG (Embedded Systems Work Group)」を設立し、自動車など組込み向けの標準化と普及活動を本格的に開始している。

TCG の EmSys WG では Infineon 社と富士通の 2 名からなる共同議長が担当している。TCG EmSys では、2.2.2 で紹介する米国運輸省の RFI (Request For Information)に対して、EVITA や IPA などの活動を含めた、現在の自動車セキュリティの取組みについて情報提供している。また、自動車業界からは 2011 年 6 月の EmSys 初回会合で EVITA プロジェクトの責任者として BMW 社から講演と情報交換が行われている。2012 年 3 月には、トヨタ自動車が TCG に加入したことを発表[22]している。

2.1.3.2　escar 2011 のプログラムから

escar 2011 では、大学から 3.1.1 で後述する Kohno 准教授の発表と、2010 年度調査 [4] で紹介したサウスカロライナ大学の TPMS (Tire Pressure Monitoring System)の問題について発表があり、参加者から多数質問があり関心をひいていた。EVITA プロジェクトと、EVITA HSM を AUTOSAR 標準に導入する仕様について発表があり、2.1.1 で紹介した。

スペインのマドリッド大学から、自動車同士が構成するアドホックネットワーク(VANET:

---

[21] TCG (Trusted Computing Group), http://www.trustedcomputinggroup.org/

[22] “トヨタ自動車株式会社、Trusted Computing Group (TCG) に加盟, http://www.trustedcomputinggroup.org/media_room/news/244

Vehicle Ad-hoc Networks)の挙動をシミュレートする VanSimFM ツールの発表があった。VANET では、接近する複数の自動車が自動的にネットワークを構成・消滅させるため、動作の予測が難しい。また、接続には無線通信を使うため、ネットワーク通信のシミュレーションのほか、電波の伝播モデルの構成も必要で、これらを組み合わせたシミュレーションは一括して実行できなかった。マドリッド大学ではオープンソースのシミュレーションツールとして CityMob、SUMO、NS-2 を統合し、一括してシミュレーションを実行できる環境を開発した。

自動車同士の直接通信による車車間通信では、セキュリティの面からも VanSimFM のようなシミュレーションツールによって想定を検証する環境は重要である。

2.1.4 ITU「Fully Networked Car」ワークショップ

ITU (International Telecommunication Union: 国際電気通信連合[23])は毎年、完全にネットワーク接続された(Fully Networked)自動車と題して 2012 年までに 7 回のワークショップを開催している。スイスで開催されるジュネーブモーターショーにあわせて、国際標準化を行っている ITU (Intelligent Transport System)、ISO (International Organization for Standardization)、IEC (International Electrotechnical Commission)が協調開催している。

このワークショップの発表者はチップメーカ、携帯電話業界、通信業界、ITS 関連業界から広く参加があり、開催後に公開されている資料から業界の動向に触れやすい。過去の資料は「Workshops on ICT in Vehicles[24]」に掲載されている。

2012 年のワークショップ[25]では、EV とモビリティ、セーフティと注意散漫、ITS 通信と標準などのセッションが開催された。ITS については情報セキュリティについても触れられた模様である。

2.2 米国の自動車情報セキュリティの動向

米国では 2010 年と 2011 年に発表されたワシントン大学 Kohno 准教授ら CAESS の研究論文[26]で自動車の情報セキュリティの問題が全般的に実証されている。

本節では米国運輸省(USDOT: United States Department of Transportation)[27]が中心に行っている ITS の普及活動に関連した情報セキュリティの動向と、USDOT が自動車の情報セキュリティについて情報を募集する呼びかけについて概要を報告する。

---

[23] ITU (International Telecommunication Union: 国際電気通信連合), http://www.itu.int/

[24] “Workshops on ICT in Vehicles”, ITU, http://www.itu.int/ITU-T/worksem/ict-auto/

[25] “THE FULLY NETWORKED CAR Workshop”, IEC, ISO, ITU, 2012-03-07
http://www.worldstandardscooperation.org/fully_networked_car2012.html

[26] “Center for Automotive Embedded Systems Security – Publications”, CAESS
http://www.autosec.org/publications.html

[27] 米国運輸省(USDOT: United States Department of Transportation), http://www.dot.gov/

2.2.1 RITA, Volpe Center の ITS 普及活動

USDOT の研究組織である RITA (The Research and Innovative Technology Administration)[28]のうち、運輸システムの革新を研究開発する部門に Volpe Center[29]がある。Volpe Center 航空・鉄道・海運・軍事輸送・自動車・ITS などの分野の技術革新を進める調査や研究開発、トレーニングを行う機関である。

Volpe Center にある 8 つあるテクニカルセンターのうちのひとつが”Center for Transportation Logistics and Security” (輸送物流とセキュリティのセンタ)である。Volpe Center は 1972 年以来、主にセーフティ面から輸送システムの研究開発を行っており、2009 年以降は海運のセキュリティやバスなど交通システムのセキュリティについても調査研究を行っている。

Volpe Center の上位組織である RITA には ITS に関して複数の部局が参加する”ITS Joint Program Office” (JPO)があり、この中で ITS の研究調査、普及活動が行われている。JPO では、T3 Webinar という Web セミナで 2011 年 12 月に交通システムの情報セキュリティに関するセミナが開催された[30]。この中で、Volpe Center の Director から、ライフサイクル全体について情報セキュリティへの対応が必要であることや、航空業界で関係者が連携して対応している例をよい実例として示している。道路交通について管轄している NHTSA (National Highway Traffic Safety Administration)[31]の講演からは、EVITA や Timed Triggered Communication Protocol など国際的なセキュリティ活動に学ぶこと、情報セキュリティ対策は NIST (National Institute of Standards and Technology)の情報セキュリティ標準に従って産業向けに展開すること、情報セキュリティの学習・評価用のシミュレータの開発などが指摘されていた。高速道路建設を技術支援する FHWA (Federal Highway Administration)からは、工事用の道路標識など現場に設置した機器の設定が書き換えられる事例、GSM (Global System for Mobile Communications)基地局がなりすましされる事例、バスのモータに対するトルク発生量の設定書き換えの事例などが紹介されていた。

政府機関である USDOT に対応する業界団体には、米国自動車技術会(SAE International: 旧略称で Society of Automobile Engineers の意)がある。SAE は自動車業界と航空業界にまたがった活動を行っており、航空機と自動車の情報セキュリティそれぞれに関連したシンポジウムなど会議も開催している[32]。航空機でも制御システムの電子化が進んでおり、本調査の研究会では自動車の情報セキュリティと共通するという指摘もあった。

---

[28] RITA: The Research and Innovative Technology Administration, http://www.rita.dot.gov/

[29] Volpe Center, http://www.volpe.dot.gov/

[30] “ITS - T3 Webinar: Introduction to Cyber Security Issues for Transportation”, RITA, ITS JPO, 2011-12-07 http://www.pcb.its.dot.gov/t3/s111207_cybersecurity.asp

[31] NHTSA: National Highway Traffic Safety Administration, http://www.nhtsa.gov/

[32] “VIIC Security”, SAE International, 2012-01-25 http://www.sae.org/servlets/techSession?EVT_NAME=G201&SCHED_NUM=198140&REQUEST_TYPE=SESSION_DETAILS&GROUP_CD=TSESS

2.2.2 米国運輸省(USDOT)によるサイバーセキュリティとセーフティに関する情報募集(RFI)

米国運輸省の研究組織である Volpe Center は 2011 年 8 月に自動車情報セキュリティ(Cyber Security)とセーフティについて、広く情報を求める募集(RFI: Request For Information)[33]を行った。この RFI が求める情報の範囲は広く、既存の宇宙・航空・医療・軍事を含めた事例や研究を含めて対策例や普及・トレーニングの方法を募集している。

自動車の情報セキュリティとセーフティの両方について、米国政府がどのような視点を持っているか整理するため RFI の概要をまとめる。

2.2.2.1 RFI の概要

RFI では、今後の研究開発を計画するための情報収集として、電子制御システムを搭載した自動車の情報セキュリティとセーフティについて情報を募集した。

2.2.2.2 背景

RFI では自動車情報セキュリティの背景を次のように説明している。「交通システムでは、セーフティの実現と燃費向上などのために電子制御の利用が増大している。情報システムと制御システムが融合し(cyber-physical system)、制御が複雑になった結果、車載システムに起因する故障や、セーフティと脆弱性に関連した未知のメカニズムが登場している。このような背景から米国運輸省は自動車情報セキュリティとセーフティについての研究を計画するものとした。」

計画では製品としての自動車の情報セキュリティに着目し、対象は自動車の制御システム、セーフティ、運転支援、省エネ、信頼性機能から、インフォテイメント、無線を含むネットワークとしている。これらの次世代の研究ステップについての戦略を提案し、既存の施策を見直す。施策としては法規制、強制力、事故調査、自動車試験、啓蒙・教育、システム構成への提案、設計の原則や実践例の普及などである。

2.2.2.3 募集する情報

募集する情報は、電子制御システムが適用された異業種についても、情報セキュリティとセーフティに関する標準、事例、判明したこと、とあり範囲が広い。

情報セキュリティについては特に、自動車、航空、軍事、生産制御、情報、通信、スマートグリッド、医療、ヘルスケアから、技術的な対策方法を募集している。また、各業界で情報セキュリティと脆弱性に注目したきっかけについても情報を求めている。

---

[33] “Cyber security and Safety of Motor Vehicles Equipped with Electronic Control Systems”, USDOT RITA, 2011-08-02
https://www.fbo.gov/index?s=opportunity&mode=form&id=cf79b1f81fb62d1dc78084e9a9fd3ace&tab=core&tabmode=list&=

2.2.2.4　情報セキュリティに関連する情報募集

情報セキュリティに関連する情報募集については以下のとおりである。情報セキュリティについては標準仕様と関連組織をどのように連携して普及させるかがポイントになっている。

(1) きっかけ: セーフティと情報セキュリティに取り組むきっかけとなる事件、事例
(2) 情報・サービス: 対策として提供された情報やサービス
(3) 組織: 業界で形成された委員会、作業グループ
(4) 標準化: 対策に使われた標準、標準への修正、新規作成の必要性
(5) 普及: 普及方法、組織・団体を巻き込んで動かす方法
(6) 規制: 政府、警察、規制当局が果たした役割
(7) 保護: 個人情報、競走上重要な情報などの保護手法

2.2.2.5　セーフティ関連への情報募集

セーフティに関連する情報については、すでに蓄積されたセーフティへの対策方法のほか、情報セキュリティの脅威に起因するセーフティへの影響についての対策方法も求めている。対象とする業界は自動車、航空、列車制御、軍事指令制御、医療機器、監視機器で、以下のようなトピックスがある。

(1) 故障・障害管理: 故障・障害と侵入に関する分析・評価・深刻度などの管理
(2) 故障・障害対策: 故障と障害の検出、侵入検知・防止、セーフティ設計などのしくみ
(3) HMI (Human Machine Interface): 運転者と自動車のやりとり、インタフェース。特に通知の戦略と、自動操作からマニュアル操作に移行する方法
(4) 記録: 診断コードと発生履歴(event history)の生成・記録
(5) 監視・保守: 動作中の監視、ライフサイクルにわたる保守の必要性
(6) 試験: 確認、検証、認定を含むシステムの試験手法
(7) 設計: システム設計の要件と設計手順
(8) 標準: 有効な標準、手順、手法、実践

2.3 日本国内の自動車情報セキュリティの動向

日本国内での自動車情報セキュリティに関する主な活動は IPA の調査研究がある。業界団体では自動車技術会とインターネット ITS 協議会の活動がある。

2.3.1 自動車の情報セキュリティに関する活動

2.3.1.1 IPA における自動車情報セキュリティの検討

IPA では 2006 年度から組込みシステムの情報セキュリティの調査の一環として、自動車に関する情報セキュリティの動向調査と、業界識者による研究会の開催、自動車業界向けの広報を行ってきた。2009 年度以降は特に欧州の研究開発動向から EVITA プロジェクトと escar カンファレンスについて動向調査と報告を行っている。2010 年には米国の大学などによる車載 LAN と無線通信の脆弱性に関する論文が複数発表され、報告で紹介している。

IPA では情報セキュリティ全般について調査分析御及び普及活動を行っており、自動車のような組込みシステムのセキュリティの他にも、交通インフラを含めた制御システムのセキュリティに関しても調査分析を行っている。一方で、通信を行う組込み機器の既知の脆弱性を検査するツールの提供や、情報セキュリティ技術者を含む情報処理技術者育成などの活動を行っている。

2.3.1.2 ITS Forum のセキュリティガイドライン

日本の ETC 方式、ITS スポットの標準を管理する ITS 情報通信システム推進会議(ITS Forum)[34]では 2011 年、DSRC を利用した運転支援通信システムに関する「運用管理ガイドライン」と「セキュリティガイドライン」を発行し公開している。主な内容について 4.2.5 で後述する。

2.3.1.3 自動車技術会

自動車技術会(JSAE: Society of Automotive Engineers of Japan, Inc.)は 2010 年から情報セキュリティに関する標準化を目指して「情報セキュリティ小委員会」で検討を行っている。

また、JSAE では ITS 関連の標準化活動に日本の業界団体の代表として参加している。情報セキュリティ関連のアイテムも含まれた ISO TC204 の進捗状況がワーキンググループ一覧などの形で公開されている。活動主体は「ITS 標準化委員会」[35]である。

---

[34] ITS 情報通信システム推進会議 (ITS Forum)
http://www.itsforum.gr.jp/

[35] “ITS 標準化委員会”, JSAE, http://www.jsae.or.jp/01info/org08.html

2.3.1.4　インターネット ITS 協議会

インターネット ITS 協議会では、自動車のプローブ情報を利活用する上での仕組みについて、そこに含まれるセキュリティ課題も含めた検討を行っている。2011 年度の活動では、自動車とクラウドをスマートフォンで繋いだシステム(図 2-4 セキュリティを考慮したプローブ情報活用モデル)を想定し、情報漏えいや悪意による攻撃に対するセキュリティ対策を踏まえた、エコドライブや利便性向上の実現に向けた技術及びシステムの開発を行っている。また、この成果を一般車道上で実証実験を行う事で、より具体的なシステムの検証を実施している。

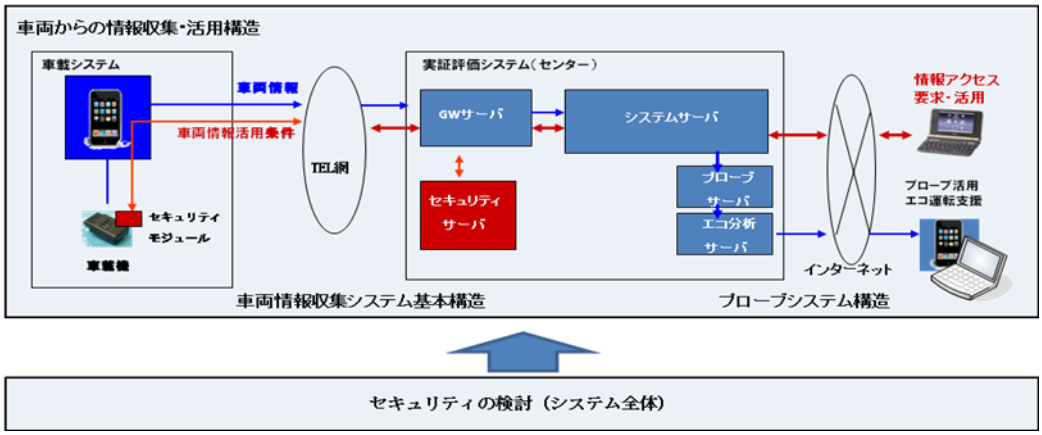

図 2-4 セキュリティを考慮したプローブ情報活用モデル

2.3.2　安全快適を実現する機能の充実

自動車の電子制御によるセーフティ機能や快適に走行させるための機能にはさまざまなものがある。例えばトヨタ自動車の「統合安全コンセプト」では、停車時から衝突、事故後に利活用する 17 種類の安全機能を提示している[36]。これまで、自動車の安全機能は個別の安全機能として提供されていたが、全てを矛盾がないように総合的に連携させ、快適な運転を実現するのが「統合安全コンセプト」である。これに似た考え方は日産自動車の「セーフティシールドパッケージ」[37]がある。

このような複雑な制御を利用する自動車の安全快適機能では、自動車の車載制御システムが必須となっており、自動車の車載制御システムが「走る・曲がる・止まる」という自動車のセーフティに直接影響する機能にも関わっている状況にある。そのため、様々な情報を車載制御システムが電子制御して、安全快適な走行を提供しようとする取組みにおいては、外部からの情報取得や、それらの情報処理について情報セキュリティ上の脅威に関しても検討を進める必要がある。

---

[36] “最先端技術の「予防安全」と「衝突安全」／統合安全コンセプト”, トヨタ自動車 http://www.toyota.co.jp/jpn/tech/safety/technology/concept/

[37] “セーフティシールドパッケージ”, 日産自動車, http://www.nissan.co.jp/FUGA/equip_advance.html

2.4 自動車情報セキュリティ動向調査のまとめ

2.4.1 着実に進む欧州の研究開発

2.1 で見たように、欧州では EVITA に続き PRESERVE という研究開発プロジェクトで ASIC 化によるセキュリティハードウェアの開発が進められている。この ASIC に搭載される EVITA セキュリティ仕様は Bosch 社などにより AUTOSAR 標準に取り込む活動も行われている。また、PRESERVE の実証実験では、数百台の実車への車載機を準備し、同時に電子証明書に関連するサーバインフラも含めて開発と試験が行われている点が先進的である。また、実証実験は米国でも予定されている。

2.4.2 自動車情報セキュリティのコミュニティ

2.2 の各国の動向を分析すると、EVITA と PRESERVE に共通する点としては、自動車業界内から人材が集まり、コミュニティで開発・実験などを行っている。また、Bosch 社のように AUTOSAR への標準化を進める企業もあり、普及に有利である。

USDOT でも自動車情報セキュリティに関する情報募集の中で業界内や政府組織での情報セキュリティを推進する動機付けや役割分担などについて情報を求めており、情報セキュリティに関するコミュニティの影響は大きい。

日本においても IPA や ITS 情報通信システム推進会議、自動車技術会等で、自動車情報セキュリティに関する検討が進められているものの、海外に比べると部分的な活動にとどまっている。今後、セキュアな自動車を検討・開発していく上では、より広い活動が求められる。

2.4.3 安全快適機能による情報と制御機能の連携

かつて自動車の排気ガス対策のために電子制御システムが導入されたように、現在の安全・快適・省エネな運転を実現するためには、2.3.2 で示したように情報システムによる安全快適機能が必須のものとなっている。ここでいう「安全快適機能」とは、自動車やスマートフォン等の持ち込み機器のセンサ情報やソフトウェアと、自動車のブレーキ、エンジン、ステアリングなどの自動車の基本制御機能を連携させることで、安全で快適な走行を目指す機能を示す。このような機能が自動車の安全性や満足度を向上させる一方で、外部接続が増えることで攻撃の口が増え、情報セキュリティ上の脅威に繋がることが予測される。また、安全快適機能が複雑化することによって、脆弱性の混入など開発段階から意識して取り組まねばならないセキュリティ上の課題も発生しかねない。情報セキュリティの「想定外」によって事故が起きないよう、「安全快適機能」のように自動車の基本制御機能に関連する処理については、情報セキュリティ上の検討が特に重要である。

3　自動車情報セキュリティの脅威の動向

本章では、3.1 に自動車の車外からの複数の侵入を総合的に示す研究論文と、その他個別の事例を紹介する。その後 3.2 で脅威の事例について分析を行う。

3.1　自動車情報セキュリティの脅威の事例

本節では、自動車情報セキュリティに関して、実際に発生した事例や研究者による実証に基づく脅威について調査を行った結果を示す。

3.1.1　自動車の外部から車載 LAN への不正侵入

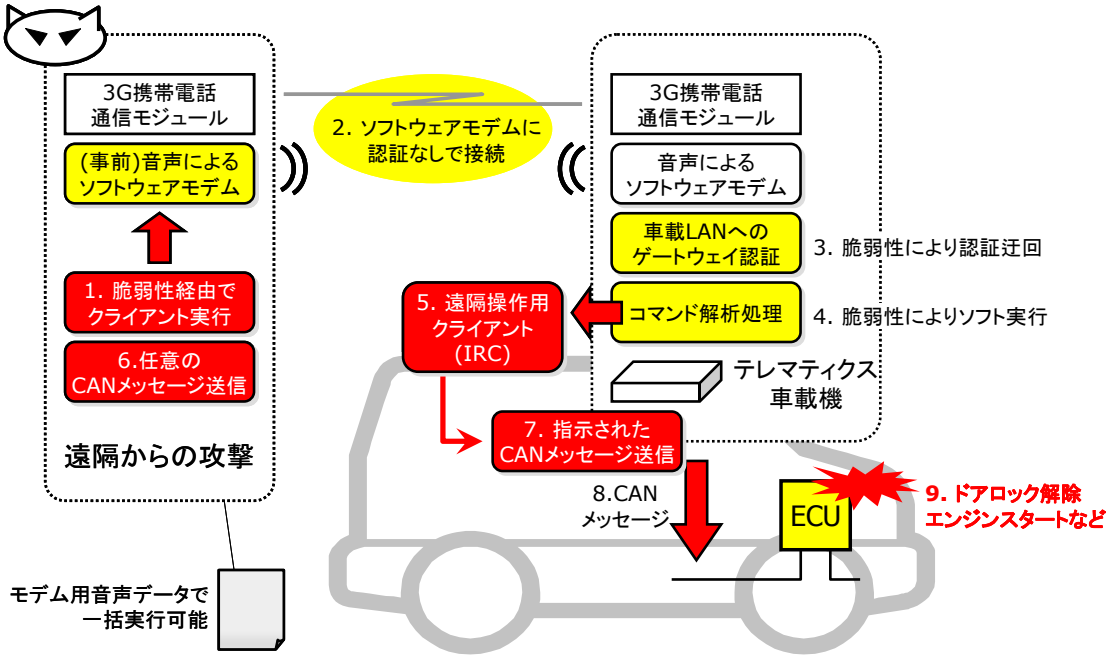

図 3-1 自動車の外部から車載 LAN への不正侵入

3.1.1.1　概要

ワシントン大学 Kohno 准教授らは、2010 年に自動車の車室内から自動車の制御システムへの攻撃を実証した。翌 2011 年の Kohno 論文では、自動車の車外から自動車に触れずに攻撃できる侵入経路を全般的に調査し、3G 携帯電話経由のほか、コンパクトディスク(CD: Compact Disc)に書かれた音楽データも含め広範囲の侵入経路(attack vector)の実証に成功した[38]。2011 年の Kohno 論文の発表では、デモを行うビデオも公開されている[39]。

[38] “Comprehensive Experimental Analyses of Automotive Attack Surfaces”, Stephen Checkoway

3.1.1.2 影響

2011 年の Kohno 論文では多数の攻撃例を実証しているが、その中でも被害が大きくなると予想される攻撃例が論文で指摘されている。論文では、自動車の盗難と、攻撃者からの車室内の監視について動機の例を示した、としている。

1. 自動車の盗難

遠隔操作によりドアを解錠できることと、遠隔地でも複数の自動車を対象にできることから、自動車窃盗行為が簡易化される可能性がある、と指摘している。

2. 車室内の監視

テレマティクスユニットの乗っ取りによって、特定の自動車に対して、音声、ビデオ、位置の記録を盗み出すことができ、個人の監視、産業スパイ、ストーカー、会話盗聴などが可能である。乗っ取りが成功した場合、インターネットを介して自動車の情報を取得することができるため、監視しやすい、と指摘している。

3.1.1.3 攻撃の難易度、制限

論文では特定テレマティクス端末内への侵入コードと実行コードが新しく開発されている。テレマティクス端末用の IPv4 アドレスの特定は、コード開発にはリバースエンジニアリングツールを利用しており専門性が高い。特定車種のテレマティクス端末に限るため全般的ではなく部分的である。ただし大手テレマティクスサービス OnStar のように数百万台に対応[40]するサービスでは攻撃可能な範囲が非常に広い。

3.1.1.4 対策

論文で提案されている対策は以下のとおりである。

1. 外部接続の制限

論文では「自動車が、外部からの不必要な通信に対してオープンであったことに驚いた」と述べている。Bluetooth の手作業でのペアリングを必須にしたり、携帯電話網との通信はテレマティクス装置の起動命令だけにする、携帯電話からは定期的に発信させるようにして着信させないようにする、などの対応方法があるとしている。

また、自動車の制御通信をそのまま中継する場合、改ざんされないように SSL などで通信メッセージを保護できるとしている。

(University of California, San Diego), 2011-08, http://www.youtube.com/watch?v=bHfOziIwXic

[39] “20th USENIX Security Symposium: Comprehensive Experimental Analyses of Automotive Attack Surfaces”, Stefan Savage, University of California, San Diego; Tadayoshi Kohno, University of Washington, etc.
http://www.usenix.org/events/sec11/tech/

[40] “GM オンスターの新サービス…盗難車を安全に停車”, レスポンス, 2009-07-22
http://response.jp/article/2009/07/22/120503.html

さらに、Bluetooth とテレマティクスの間のように重要な通信を行うチャンネルでは監視を行うよう勧めている。例えば一定回数以上の連続した認証失敗に対しては一定時間応答しないようにし、特定のインターネット上のあて先に対しては通信を遮断することを勧めている。

このほか、ECU のフラッシュ書き換える手順を限定して攻撃経路を減らす方法、ECU 上で不要な通信サービス（例えば FTP (File Transfer Protocol)など）の機能を削除する対策が提案されている。

2. セキュアな開発手法を利用する

脆弱性を排除するためにセキュアなツールの利用、セキュアプログラミングの利用を指摘している。例えば`strcpy`のような脆弱性を含む関数を使わない、入力値の検査を行う、モジュール間の接続時に行うべき処理を明確にすることなどが指摘されている。

また、攻撃者に攻撃の糸口を与えないため、製品段階の ECU に実装するコードからは、すべてのデバッグシンボルとエラー文字列を削除するよう指摘している。

3. セキュアなソフトウェア更新方法を実装する

ソフトウェアの更新は安全なソフトウェアであり続けるために必須だが、更新時に悪意のあるソフトウェアに書き換えられないようにする必要がある。そのためには、メーカによるソフトウェアの更新を適切に実行できるなどの要件を検討し、実装することが必要だとしている。

4. 機能と機能をつなぐソフトウェアにはより慎重なセキュリティ対策の検討が必要

脆弱性は最新のコード内ではなく、旧来の機能と最新の機能の間の接合部に見つかっている。これは互いに充分に機能を理解せずに他の機能を呼び出しているためである。メディアプレーヤのソフトを CD で更新する機能は車載オーディオ機によくある機能だが[41]、今回の CD ベースのソフト更新処理の脆弱性については正しいソフトウェアで更新しようとしているかなど、更新処理の検証を行っていないことが考えられる。

自動車の様々な部品をまたがるソフトウェアを開発する場合、それらを統合した上でのセキュリティ分析とレビューが必要だが、部品メーカはソースコードを出せないため難しい。自動車の産業界の中で、さまざまな情報セキュリティ対策を併用したり組み合わせて利用できるよう、互換性を保つことがひとつの対策として考えられる。そのためにもコンピュータセキュリティ業界と自動車業界がより緊密になることが求められる、としめくくっている。

[41] 車載オーディオの業界関係者へのヒアリングによる, 2012-03

3.1.2　車載サーバからビデオの記録が漏洩する問題

米国で、ある自治体の警察用パトロールカーのビデオレコーダの映像記録が、車載の無線 LAN アクセスポイントと FTP サーバを経由して漏洩する問題があった[42]。なお、この件は情報セキュリティを調査する会社により指摘された問題である。

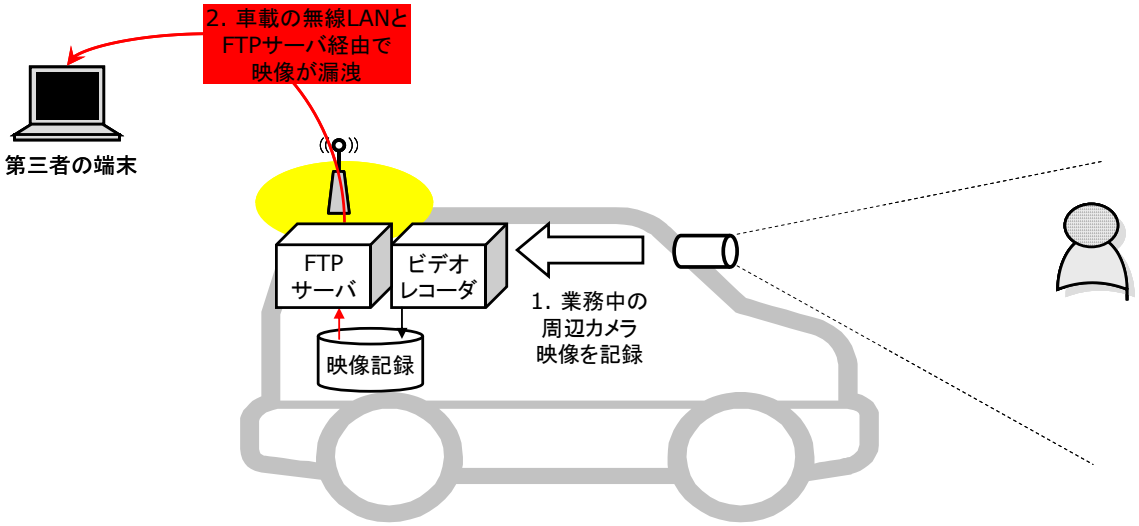

図 3-2 パトロールカーのビデオレコーダの映像記録が漏洩する問題

3.1.2.1　原因

このパトロールカーでは業務中の周辺映像を記録するため、パトロールカーがビデオレコーダを搭載して記録していた。調査会社の指摘によれば、この車載ビデオレコーダの記録映像は、内蔵している FTP サーバを通じて認証なしで取り出せるようになっていることが原因だった。

3.1.2.2　影響

図 3-2 のようにパトロールカーの記録映像には、停車させられた自動車のナンバープレートや、取り締まりを受けた市民の顔なども含まれることが考えられる。これによって、プライバシ情報の漏えいや、犯罪等への関与とうの誤解に繋がる可能性がある。

---

[42] “Hacker pwns police cruiser and lives to tell tale”, The Register, 2011-05-03
http://www.theregister.co.uk/2011/05/03/cop_car_hacking/
“Caution: Malware Ahead An analysis of emerging risks in automotive system security”, McAfee, 2011-05
http://www.mcafee.com/us/resources/reports/rp-caution-malware-ahead.pdf

3.1.2.3　攻撃の難易度、制限

無線 LAN の SSID (Service Set Identifier)のスキャンや、ポートのスキャンなどを行えるツールを使って簡単に実行できるため難易度は低い。ただし、影響する範囲は特定のパトロールカーと無線 LAN で通信できる範囲内に限られる。

3.1.2.4　対策

利用者は車載の FTP サーバに適切なパスワードを設定することが適切である。

システム上の対策としては、パスワード設定手順か認証手順の改善、FTP サーバへのアクセス制限、映像の格納先の選択など、複数の検討案が考えられる。

3.1.3　RF ジャマーによる自動車の盗難

自動車の盗難防止技術などの情報を掲載した SBD Japan 社の日本語情報誌[43]によれば、南アフリカで「RF ブロック」または「RF ジャマー (jammer)」を使った盗難が増加しているとのことである。RF ジャマーは自動車のスマートキーが使う周波数と同じ周波数を発する家庭用の一般的なリモコンを使ってスマートキーからの電波による信号を妨害する手口である。

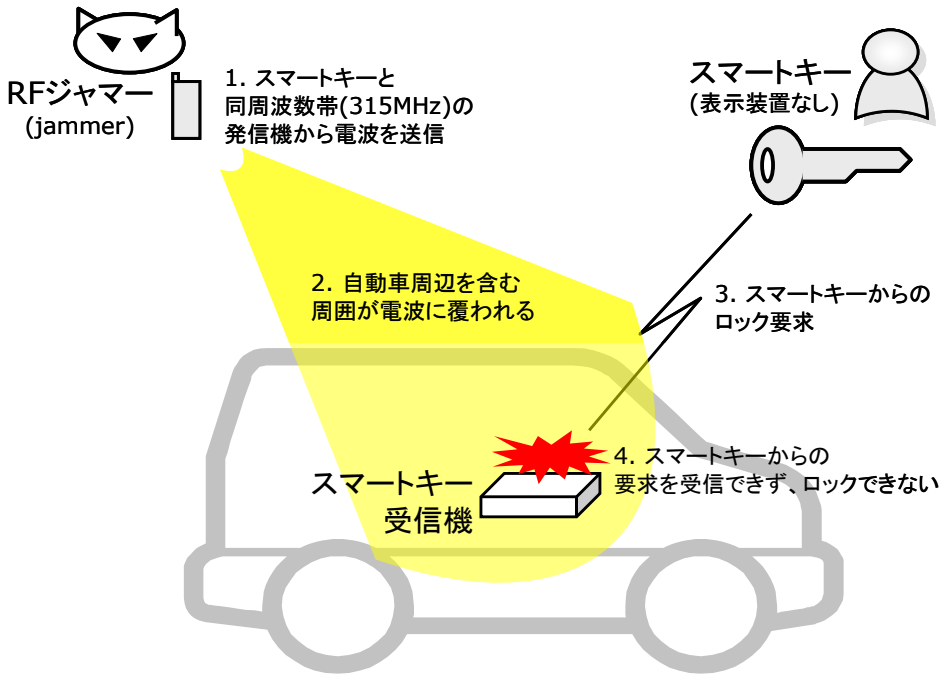

図 3-3 RF ジャマーによる自動車の盗難

[43] “Secure Car Newsletter 2012 年 2 月”, SBD Japan, 2012-02
http://www.sbdjapan.co.jp/jpnews/file.axd?file=2012%2f3%2fSecure_Car_Newsletter_Feb_2012_J.pdf

3.1.3.1 原因

自動車のスマートキーで利用される電波の周波数は電波利用の免許なしで運用でき、産業機器や家電を含む他の機器でも利用されていることがある。そのためスマートキーを使う自動車の近くで同じ周波数の電波を放射されることでスマートキーが一時的に使えなくなることがある。

また、スマートキーではドアロックが完了したことを示す表示は自動車のウィンカーの点滅などであり、スマートキーには表示や振動などのフィードバックがないため、自動車を目視して確認しなければドアロックが完了したかどうかわからない。慣れによって自動車のウィンカー表示を確認せず、スマートキーを操作しただけでドアロックができたと思い込んだときに、攻撃者による侵入可能な余地ができる。

3.1.3.2 影響

スマートキーから自動車の方向への電波は 315MHz 帯で、サウスカロライナ大学での実験では 200〜300m でも通信できると指摘する論文があるため、駐車場の周辺にある建物や物陰から妨害される可能性がある。攻撃の対象になりやすいのは高級車または人気車種であると考えられる。

3.1.3.3 攻撃の難易度、制限

315MHz 帯は産業用機器、テレメータ機器などで電波を無免許で利用できるよう認可されているため関連機器がよく普及している。南アフリカの例では RF ジャマーを行うための機器は家庭用、とあり入手しやすい。日本国内ではラジコン用に市販されている例があり、ほぼ連続的に電波を放射でき、スマートキーの電波通信の妨害に悪用しやすい。

ドアロックを妨害したあと、自動車の室内に入って自動車を窃取する手法については専門知識が必要だが、窃盗や車上あらし等の攻撃の糸口とするためには有効な攻撃手法である。

3.1.3.4 対策

自動車の利用者はドアロックができたことを、目視でウィンカーを確認するか、ドアノブを操作するなどして確認すればよい。または 315MHz 帯の電波を使うスマートキーではなく、車載の携帯電話通信など別の通信方式を利用したスマートキーシステムを利用するか、スマートキー自体を使わない対策がある。

スマートキー製品としては、ドアロックが完了したか、ドアロックが失敗したことを示すフィードバック機能を自動車のキーに提供する方法がある。ただしフィードバックを自動車のキーに返すには、現在の LF (Low Frequency)帯の周波数では通信できる距離が短いため別の通信方法が必要である。

3.1.4　偽の GPS 信号により位置をだまされる問題

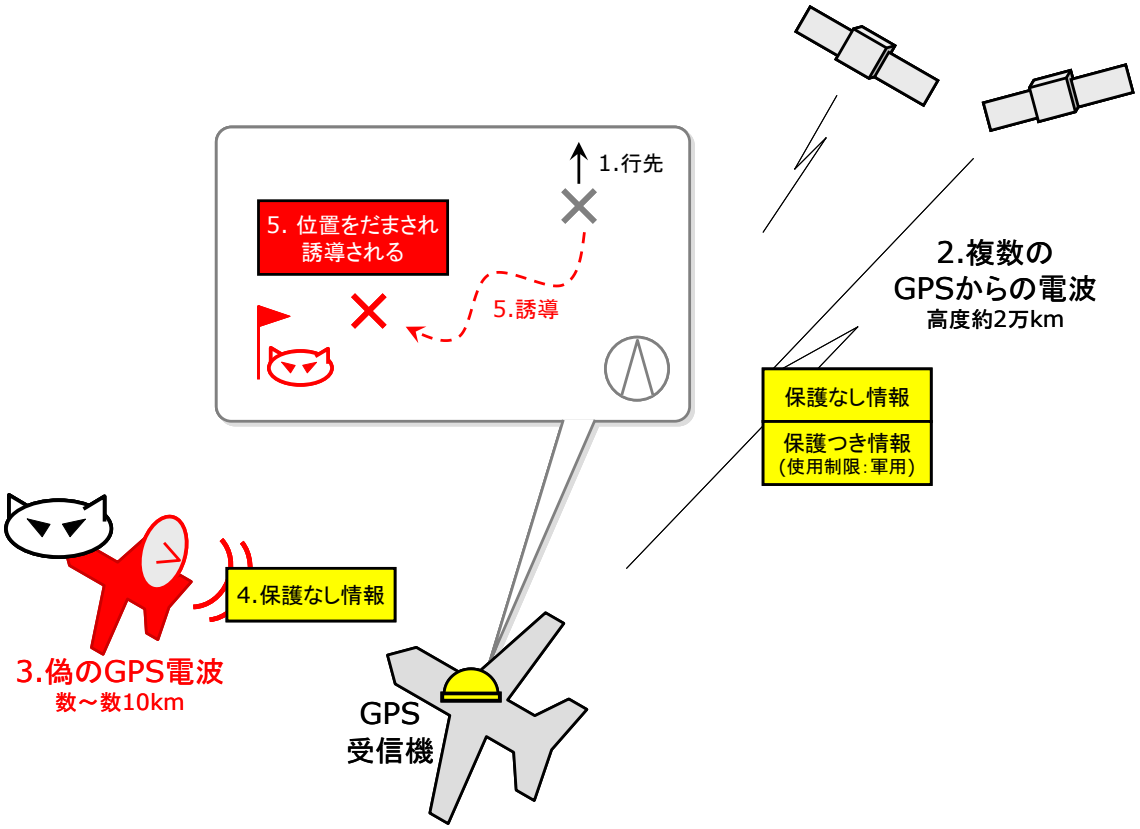

図 3-4 偽の GPS 信号により位置をだまされる問題

2011 年、イラン上空を偵察飛行していた米国の無人偵察機(UAV: Unmanned Air Vehicle) RQ-170 Sentinel が、イランによる偽の GPS (Global Positioning System)信号によって位置をだまされてイラン国内に着陸させられる問題があった[44]。イランは、遠隔操縦を行う無線通信を妨害して無人偵察機を自動操縦モードに移行させ、偽の GPS 信号によって無人偵察機をイラン国内に誘導したという。

この問題は直接自動車の制御には影響しないが、GPS はカーナビやテレマティクスなど複数のサービスで重要な役割を持っているため紹介する。

3.1.4.1　原因

詳細は不明だが、この無人偵察機が GPS からの電波のうち暗号化されていない民間用の信号を使って位置情報を得ていた場合、イランが用意した別の装置から偽の GPS 信号が与えられて誘導された可能性がある。これについて米軍は否定している。

---

[44] Exclusive: Iran hijacked US drone, says Iranian engineer, 2011-12-15
http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video

3.1.4.2 影響

一般的に自動車では GPS からの位置情報だけを使って走行や停止、操舵の制御は行っていないためセーフティへの影響はないと考えられる。ただし無人の農作業車や、超大型ダンプトラックの無人運転[45]などで主に GPS を利用して運転制御している場合がある。

偽の GPS 情報を受け入れてしまうと、カーナビは正しく動作しない可能性がある。また、テレマティクスでは間違った位置情報がセンタにアップロードされることで、自動車の配車管理ができなくなる、盗難車の追尾ができなくなるなどの影響が考えられる。

3.1.4.3 攻撃の難易度、制限

偽の GPS 信号によって誘導を行うためには、複数の衛星に似せた GPS 信号を精密な時刻の差で同時に生成する必要がある。このような装置は GPS 信号を受信して利用する機器の試験用装置として販売されており入手は可能である。価格は 2011 年現在では数百万円程度である。ただし、GPS 衛星になりすます攻撃や GPS 端末の動作を妨害する攻撃は GPS に似せた電波が届く範囲に限られる。なりすました GPS 信号によって誘導が成功する範囲については現在のところ未確認である。

なお、米国では GPS による位置の追尾は個人情報に関わる問題であるとして、GPS が使用している電波を妨害する装置がすでに 30 ドル程度で販売されており問題であると、米国運輸省の研究組織のひとつ、Volpe Center が指摘している[46][47]。また、米国では GPS 端末が利用する周波数帯に対し、Lightsquared 社の全米無線ブロードバンド用の免許済みの電波が干渉を与えてしまう問題がある[48]。米国内での GPS の問題については GPS.gov[49]が詳しい。

3.1.4.4 対策

少なくとも GPS だけに依存した自動航法や自動運転には、特定の地域内でだまされる脅威が存在する。自動運転を行う際は GPS 以外の手段を併用して周囲の認識を行って、自動運転の速度を抑制したり停止するなど、GPS への脅威による被害の緩和にむけた対策が必要である。また、可能であれば暗号化された米軍専用の GPS 信号を使うか、GPS 以外の衛星航法システムを利用して信号のなりすましを防ぐ、暗号化などの手法を利用する。

---

[45] “無人ダンプトラック運行システム AHS（Autonomous Haulage System）”, http://www.komatsu.co.jp/CompanyInfo/profile/product_supports/

[46] “Small Jammers Present Big Problems for GPS”, Karen Van Dyke, Volpe Center, 2011-10-31 http://www.volpe.dot.gov/noteworthy/index.html#sjpbp

[47] [ビデオ] “Recent Developments in Positioning, Navigation and Timing”, Karen Van Dyke, 2011-09-27 http://www.volpe.dot.gov/media/tc/trajectories/karenvandyke.html

[48] “LightSquared、FCC に全米無線ブロードバンド計画の改訂案を提出”, 日経 ITPro, 2011-07-01 http://itpro.nikkeibp.co.jp/article/NEWS/20110701/361955/

[49] GPS.gov: Official U.S. Government information about the Global Positioning System (GPS) and related topics, http://gps.gov/

3.1.5　GSM 端末が偽の基地局に盗聴される問題

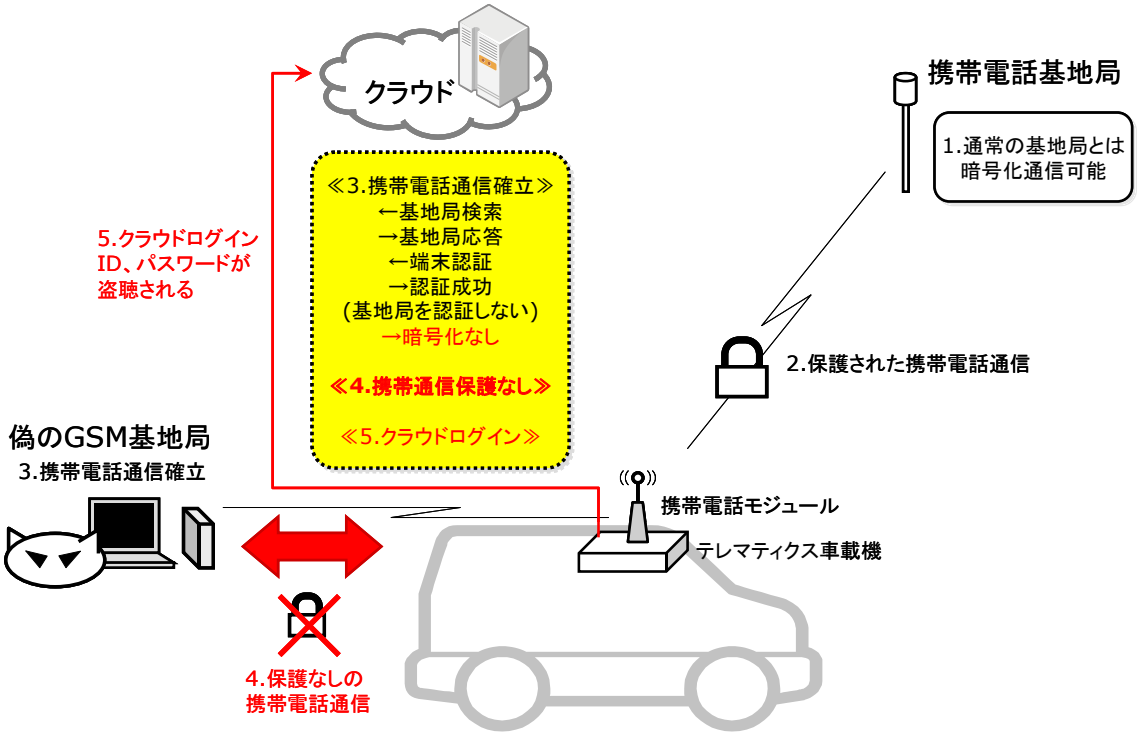

図 3-5 GSM 端末が偽の基地局に盗聴される問題

2011 年 8 月に開催された米国のセキュリティ会議「BlackHat」で、偽の GSM 基地局を使って、車載端末の GSM 認証手順を盗聴し、テキストメッセージを使って自動車のドアロックを解錠し、エンジンをスタートできたという発表があった[50]。

その 1 年前の 2010 年 8 月、米国「DEFCON 18」では約 1,500 ドルで GSM (Global System for Mobile Communications)携帯電話の基地局になりすまして、GSM 端末から発呼された音声通話を盗聴する発表が行われた[51]。この手順は IMSI-catcher として知られている。

3.1.5.1　原因

GSM 端末が偽の GSM 基地局に接続してしまう原因は主に GSM 方式で端末が基地局を認証しないことによる。GSM は第 2 世代(2G)と呼ばれる旧世代の携帯電話通信方式であり、3G や 4G のような認証手順は利用されていない。その他の付随した原因を含めると以下の点が挙げられる。

---

[50] “Hackers break into Subaru Outback via text message”, engadget, 2011-08-04
http://www.engadget.com/2011/08/04/hackers-break-into-subaru-outback-via-text-message/
“How to unlock a car with a text message”, CNN, 2011-08-03
http://edition.cnn.com/2011/TECH/mobile/08/03/black.hat.war.texting/index.html

[51] “Defcon 18 - Practical Cellphone Spying - Chris Paget - Part.mov”, killab66661, 2010-8-1
http://www.youtube.com/watch?v=DU8hg4FTm0g

(1) GSM は電波が強い基地局に接続する
(2) GSM では端末が正しいかどうか認証するが、基地局の認証は行わない
(3) GSM では基地局が暗号化の有無などの通信条件を指示する
(4) 国や地域によっては暗号化が禁止されている場合がある
(5) GSM では通信路の暗号化を行わなくても、事業者の端末への設定によって警告なしで接続する場合がある
(6) GSM 端末が通信を暗号化しない問題は携帯電話事業者の運用や、国や地域の規制により明示的に行われる場合がある

3.1.5.2 影響

日本では GSM 方式を使った携帯電話サービスは展開されていないが、海外においては中国、インドなども含めて広範囲にわたって現在もサービスが提供されている。また、GSM 方式は携帯電話だけでなく、テレマティクスなど車載用や、工場や発電所などの遠隔監視にも多数利用されている。

車載端末の GSM 通信を盗聴できる問題について BlackHat の発表者は CNN のインタビューに対して「電話や電力、交通システムを制御するシステムで GSM が広範囲に利用されていることこそが脅威である」と語っている[52]。

GSM 端末が真正な基地局に接続していた場合でも、事業者の方針や地域の規制により通信路を暗号化していない場合[53]、GSM 携帯電話システム上での通信が GSM 復調装置によって盗聴される場合がある。

3.1.5.3 攻撃の難易度、制限

2010 年の DEFCON 18 の発表では、ソフトウェアで駆動できる無線装置(USRP: Universal Software Radio Peripheral)を使って基地局装置を開発しており、コストは 1,500 ドル程度ではあるが開発の難易度は高い。GSM 基地局として動作するソフトウェアには OpenBTS[54] というオープンソースがある。

偽装した基地局によって接続できる端末は無線電波の強さや周囲の環境により、特定の範囲内に限られる。また、IMSI-catcher の方法では携帯端末から発信する信号ならば盗聴可能だが、真正な基地局が発信する信号の盗聴は難易度が高い。

---

[52] “How to unlock a car with a text message”, CNN, 2011-08-03
http://edition.cnn.com/2011/TECH/mobile/08/03/black.hat.war.texting/index.html?iref=allsearch

[53] “Hacker to Demonstrate 'Weak' Mobile Internet Security”, New York Times, 2011-08-09
http://www.nytimes.com/2011/08/10/technology/hacker-to-demonstrate-weak-mobile-internet-security.html?_r=1

[54] “OpenBTS”, Range Networks, 2011, http://openbts.sourceforge.net/

3.1.5.4　対策

DEFCON 18 の発表者は対策として 3G 以降では偽装基地局に端末を接続させたり盗聴することは難しいとし、2G を使わず 3G または 4G を使うことを勧めている。2G を使わせないように、2G の電波を妨害することもアイデアとして提示している。

USDOT の FHWA によるセミナ資料[55]によれば、2011 年の DEFCON 19 では、GSM 以外の 3G(CDMA 方式)と 4G (LTE 方式)端末に対して偽装した基地局を動作させたという[56]。この詳細は未確認ではあるが、3G/4G についても時代の変化によって脆弱性が発見されることもあるため、今後も動向に注意が必要だと考えられる。

GSM 携帯電話システム上での通信については偽装した基地局の問題以外にも、事業者や地域の規制などによる暗号化などで保護されない場合があるため、GSM 携帯電話システムを利用するアプリケーションで TLS (Transport Layer Security)や IPsec またはコンテンツ暗号化などの対策を実施することも考えられる。

3.2　自動車情報セキュリティの脅威の事例の分析

3.2.1　継続する無線接続の問題

3.2.1.1　無線接続への過度に偏った信頼は危険

2010 年度調査 [4] では OBD-II を使った有線接続による攻撃手法の研究論文が含まれていたが、本調査ではほぼすべてが無線接続による攻撃手法となった。自動車の接続方式については 2011 年の Kohno 論文で報告されたように、3G 携帯電話を使った接続についても侵入が可能であった。GSM 携帯電話の問題や GPS 衛星航法システムの問題も含めて考えれば、「絶対に安心できるものはない」ということがわかる。

3.2.1.2　無線接続の信頼性に見合った利用を

Codenomicon 社による Bluetooth の脆弱性と無線 LAN の脆弱性についてはすでに数年前から報告されている[57]が、スマートフォンの普及などにより Bluetooth や無線 LAN は自動車においても必須の接続方式の一つであることは間違いない。

しかし、人命に関わるような重要な自動車の制御機能と情報システムを連動する場合は、その通信経路の信頼性を充分に考慮したシステム設計を行う必要がある。例えば、データ

---

[55] “Cyber Concerns for Transportation Organizations – an Overview”, FHWA Resource Center in San Francisco, Edward Fok, 2011-12-07
http://www.pcb.its.dot.gov/t3/s111207/s111207_fok_presentation.pdf

[56] “DEF CON 19 - hackers get hacked!”, coderman, 2011-08-10,
http://seclists.org/fulldisclosure/2011/Aug/76

[57] “Wireless Security Past, Present and Future”, CODENOMICON, 2008-02-01
http://www.codenomicon.com/resources/whitepapers/Codenomicon_Wireless_WP_v1_0.pdf

通信機能を搭載する携帯電話モジュールを経由した命令を受け取る機能や実行する機能には､他のソフトウェアと比較して特に十分な情報セキュリティの検討と対策が必要である。また、Bluetooth や無線 LAN の接続を自動車の重要な機能から分離して動作させることや、自動車の重要な機能の制御に直接利用しないなど、無線接続の信頼性とそれを利用するサービスの内容を比較して、情報セキュリティの検討を進める必要がある。

3.2.2 車載制御システムへの攻撃の動機

本調査では自動車の情報セキュリティに関する具体的な被害例の公開情報は見当たらなかった。自動車関連の Web サイトに関しては顧客情報の流出などの事件があったが、他の大手ゲームサイトでの顧客情報流出などと同様の Web サイト側の問題と考えられる。

自動車への攻撃被害例が見当たらない背景として、自動車の車載制御システムが依然として CAN や LIN など自動車特有な車載 LAN を使用しており、インターネット対応の情報機器などよりも閉鎖的な技術を利用しているため、攻撃の難易度がやや高く、攻撃の動機が抑えられているものと考えられる。

また、制御システムを狙った Stuxnet の事例や国会や防衛産業も狙う標的型攻撃の事例も複数あったが、自動車単体についてはこれらの攻撃事例にあるほどの攻撃成果を得られないため、動機が抑えられていると考えられる。

上記のことから現状では、複数の自動車へのサービスを提供するインターネット上のサーバやクラウド、特に大規模なサイトが攻撃される可能性が高いと考えられる。車載制御システムとしては少なくとも、サービスを利用するために接続するサーバはクラウドが攻撃されて被害にあうことも想定したセキュリティ対策が求められる。

4　自動車におけるネットワーク接続の動向

2010 年度調査[4]では自動車の外部への接続方法が多様化していることと、それらが利用者を含む関係者に把握されているかが課題となった。

本章では自動車の外部との接続手法において代表的な技術及び事例をについて記載すると共に、情報セキュリティに関連する動向を整理する。

4.1　自動車のネットワーク接続の特定方法

自動車におけるネットワーク接続は必須の機能で、多様である。ここでは主にネットワーク接続で接続できる距離から図 4-1 のようなカテゴリを設定し、これに図 4-2 のような車載制御システム上での機能分類を設定し、漏れがないようにネットワーク接続を列挙した。

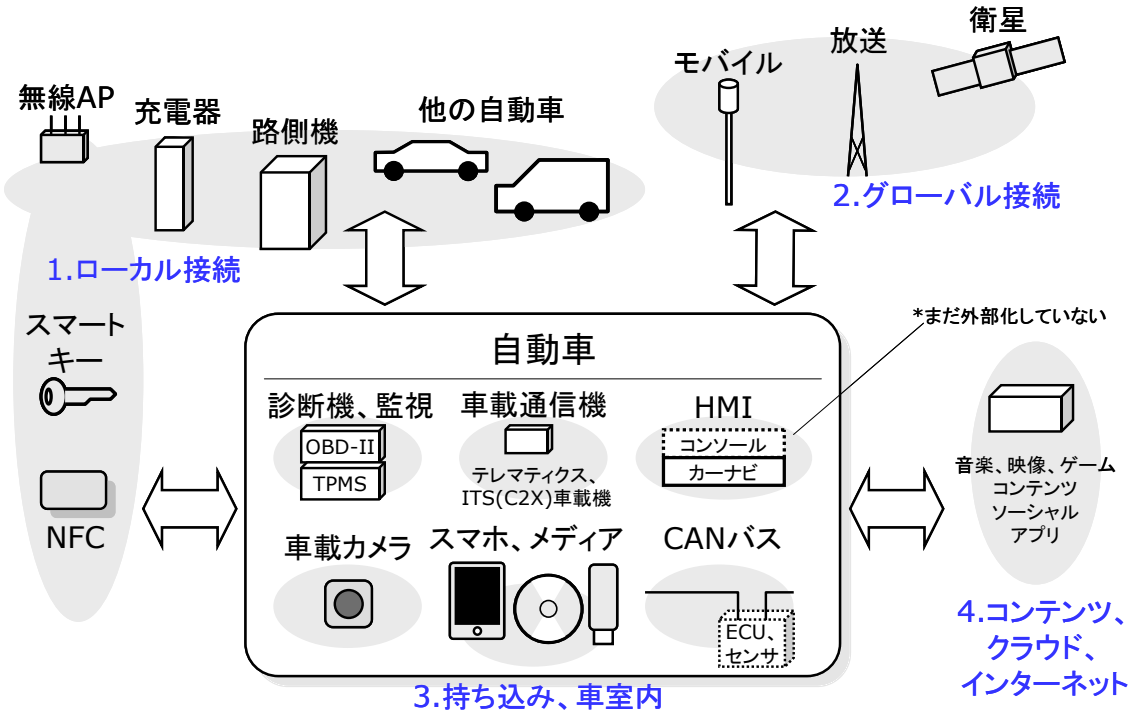

図 4-1 自動車のネットワーク接続手法の概要

図 4-1 の左側と上にある、「1.ローカル接続」、「2.グローバル接続」は無線接続の距離が 1km 未満か、1km 以上かで分類したもので、明らかに自動車の外側にある接続である。図 4-1 中央下にある「3.持ち込み、車室内」は自動車の車室内ではあるが、自動車の外側から持ち込まれる機器が接続されるため事実上の自動車の外部だと考えられる。車室内で接続できるネットワークには、車室内に露出可能な車載 LAN を含んでいる。また、「2.

持ち込み、車室内」の左上にある TPMS についてはタイヤと車載機で構成されるが、無線で通信を行うことと盗聴を実証した事例もあるため[4]事実上の自動車の外部とみなす。なお、USB (Universal Serial Bus)接続する機器や CD/DVD メディアについては一般にネットワーク接続とは言えないが、情報システムではコンピュータウイルスに感染する典型的な経路のひとつであるため、自動車の外部と接続する手法の一つとして「ネットワーク接続」に含めている。

「4.コンテンツ、クラウド、インターネット」は 1～3 のネットワーク接続上で交換されるデータに当たり、直接的に「ネットワーク接続」ではないが、スマートフォンと車載機のように API を通じて機器同士が連携動作を行う傾向が強いためネットワーク接続に含めた。

以下では、このうち大きな変化があるネットワーク接続の状況について報告する。

4.2 車載制御システムを支える車載 LAN

ここでは、ネットワーク接続手法を整理するために車載制御システムの基幹をなすネットワークを「車載 LAN」と呼ぶこととする。車載 LAN には車載の ECU やセンサ、アクチュエータ、情報機器などが接続され、車載 LAN 上で相互に通信を行う。以下にその概要を示す。

4.2.1 車載 LAN の整理

IPA では図 4-2 のように自動車の機能とそれをつなぐネットワークを整理した。

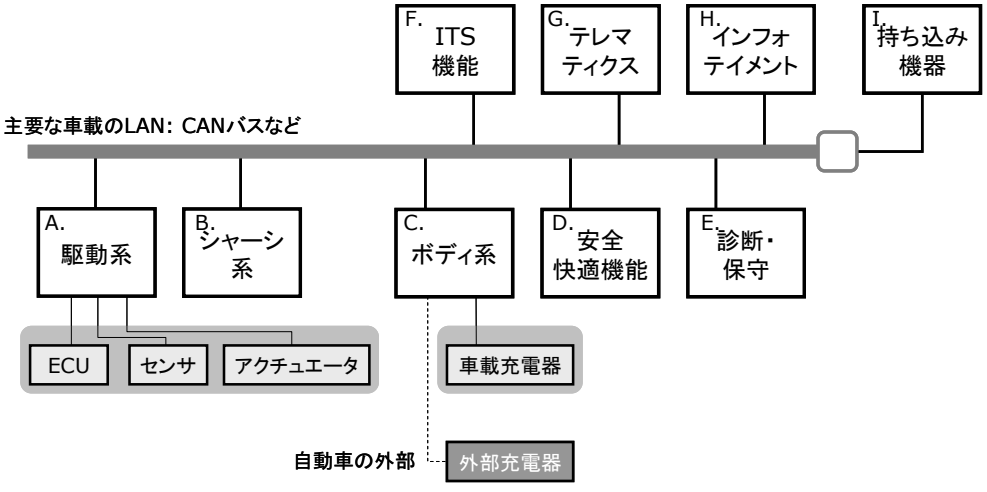

図 4-2 ネットワーク接続手法を整理するための抽象化した車載 LAN の構造

自動車のネットワーク接続手法は非常に多様で、今後も追加更新が進むと考えられる。そこで、ネットワーク接続手法を整理するために車載 LAN を最大限に抽象化し、図 4-2 の図中中央の太線ように 1 本の線で表現した。図 4-2 の下側は主に標準的に自動車に搭載

されている機能で、ECU、センサ、アクチュエータにも直接的、間接的に接続している。これらの機能は一部が規制によって技術基準が標準化されていたり、搭載が義務化されていたりするものである。図 4-2 の上側は主に自動車にオプションとして提供されたり、利用者があとから追加して搭載する機能として整理した。

これらの機能を相互に接続する機能が、図 4-2 中央の横の太線にある車載 LAN である。車載 LAN には複数の種類と複数のネットワークに分かれているが、安全快適機能を実現するために複雑に相互接続している。ここでは整理を簡単にするために車載 LAN の種類の別や数は考えないことにしている。

これまでの車載 LAN の構成図では、特に重要な部分の図示がなく、情報セキュリティの取組みをどこから着手すればよいかわかりにくかった。そのため、自動車のもっとも重要な機能から情報セキュリティ的な検討ができるよう、次のような機能の分類と優先度付けを試みた。

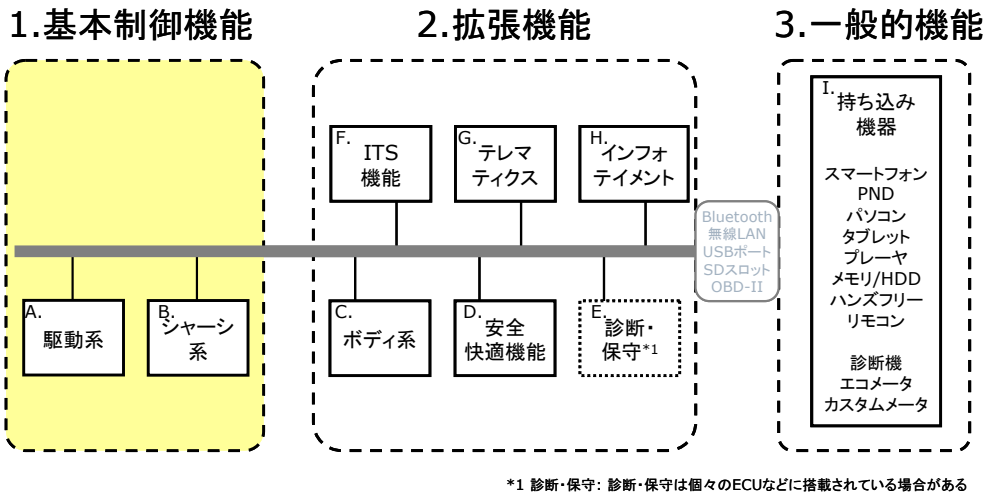

図 4-3 車載 LAN の重要度別機能分類の例

図 4-3 では、自動車を利用する上での機能の整理として、大きく「1.基本制御機能」「2.拡張機能」「3.一般的機能」に分けた。

「1.基本制御機能」は自動車の基本かつ必須の機能である「走る・曲がる・止まる」機能にあたり、セーフティに全面的に影響する。「2.拡張機能」はセーフティ確保を含めた運転支援及び快適性向上のための機能で、それぞれについて情報セキュリティ的な被害を受けた場合には個別に停止または車載制御システムから遮断してもかまわないと考えられる機能である。「3.一般的機能」は自動車の外部からの持ち込み機器からなり、ほとんどが自動車用ではない一般的な情報家電機器などである。

図 4-3 では、左にある基本制御機能を情報セキュリティの脅威から優先的に保護することが求められる。拡張機能にはドアロックなどを含むボディ系機能など重要な機能はあるが、「走る・曲がる・止まる」機能には直接影響しない。一般的機能は現在のところ自動

車の基本制御機能に該当するような機能はない。このように整理することで、多様化・複雑化した自動車のネットワーク接続に対して検討対象の優先度づけや作業分担が行いやすくなると考えられる。

なお、図 4-3 中の A～I までの機能分類の概要は以下のとおりである。

表 4-1 機能分類の概要

機能分類	機能分類	機能の一覧
1.基本制御機能	A.駆動系	エンジンやモータ、燃料・電池、トランスミッションの制御など「走る」に関する機能
	B.シャーシ系	ブレーキやステアリングの制御など「曲がる・止まる」に関する機能
2.拡張機能	C.ボディ系	ドアロック、エアコン、ライト、ウインカなど車体に関する機能
	D.安全快適機能	自動ブレーキ、車線維持制御、車間距離制御など制御機能の連携により、自動的に安全性や快適な運転を実現する機能
	E.診断・保守	OBD-II による故障診断・保守などの機能
	F. ITS 機能	ETC や ITS スポットなど路側機や車車間通信によって実現する機能
	G.テレマティクス	携帯電話網などの通信機能による位置情報収集や遠隔サービス機能
	H.インフォテイメント	カーナビ、オーディオ機器、その他、搭乗者に対する娯楽や情報提供を行う機能
3.一般的機能	I.持ち込み機器	スマートフォンや携帯型カーナビ、エコメータなど車内に持ち込む機器による機能

4.2.2 主な車載 LAN としての CAN バスと外部接続

車載 LAN のうち駆動系、シャーシ系、ボディ系などにも接続する主要な車載 LAN には CAN バスがある(図 4-2 の A, B, C)。CAN バスは現在の自動車の多くに搭載されており、運転席足元のカーペットの下などに、ECU に配線された状態で設置されていることがよくある。そのため CAN バスの配線は利用者や保守者からもアクセスしやすく、追加部品を装着するために CAN バスの配線が直接利用されることもある。

CAN バスの通信方式は電気的なレベルでは標準化されているが、要求命令や応答の内容など通信内容の意味についてはメーカごとに異なることが多く、利活用の障壁となっていた。しかし現在、CAN バスの通信内容を Bluetooth や Wi-Fi などに変換するアダプタ[58]や機能[59]が販売される例があり、CAN バスへの接続は容易になりつつある。

---

[58] “ELM327 – OBD to RS232 Interpreter”, Elm Electronics, http://elmelectronics.com/DSheets/ELM327DS.pdf

[59] “プリウス PHV、ついに市場投入, 「つながるクルマ」がいよいよ現実に”, MOTOR DAYS, 2011-12-03 http://www.motordays.com/news/articles/prius_phv_toyota_news_20111203/

車載の CAN バスは複数の本数があり、図 1-1 のように駆動系用、シャーシ系用などに CAN バスが分かれているため、CAN バスに装着した機器が直接的に車載制御システムのすべてと通信はできないが、2.3.2 で示した安全快適機能のために間接的に通信できることが多い(図 4-2 の D.)。そのため、CAN バスに任意の機器を接続して通信が可能となっている状況では、後述するようにさまざまな脅威が存在する。

4.2.3 EV 充電制御インタフェースの接続

EV、PHV (Plug-in Hybrid Vehicle)では車載の駆動用電池に充電(以下、EV 充電)を行うことができる。EV 充電制御インタフェースは、車載の駆動用電池に、自動車の車外の充電ステーションから直流電源を受けて安全かつ最低な充電を行うための接続方式と制御手順である(図 4-2 の C)。

EV 充電のための直流電源は急速充電を行うため 100 アンペアを超える電流を使う。人が感電すると生死に関わるため安全な制御が必要であり、充電制御の通信には情報セキュリティ上の配慮が必要である。

4.2.3.1 CHAdeMO 仕様の特徴

CHAdeMO[60]は自動車メーカを中心とする電気自動車(EV)の充電制御インタフェース標準化団体である。2010 年度の自動車情報セキュリティ [4] でも概要を紹介したが、2011 年になって、CHAdeMO の EV 充電時の通信手順と電力の制御手順が公開され、充電時の安全性への配慮が示されていることがわかるため、改めて紹介する。

[60] CHAdeMO 協議会, http://www.chademo.com/jp/

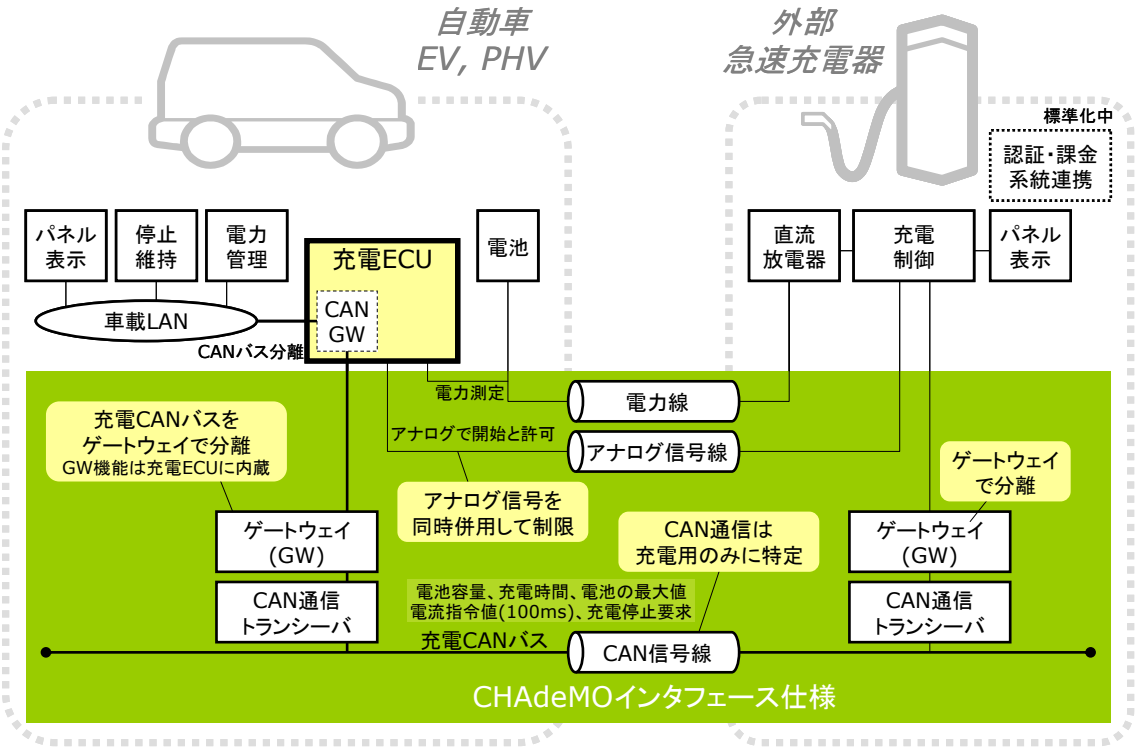

図 4-4 CHAdeMO インタフェース仕様と接続例

図 4-4 は左側に充電が必要な EV または PHV があり、図の右側に充電用の電力を供給する外部急速充電器が配置され、図の下側に CHAdeMO 仕様のインタフェース構成概要を示している。

CHAdeMO の充電制御手順は直流電源での充電時に利用される。家庭用電源から交流電源で充電する場合は交流電源用のコネクタを EV に接続して車載の充電器が対応した処理を行うため、交流電源を供給する家庭用電源コンセントの間では通信は利用しない。直流電源での充電時は CHAdeMO 仕様に対応した充電ステーション(外部急速充電器)が 100 アンペアを超える直流電流を EV に供給する。このとき、EV の充電 ECU が適切な電流量を計算して充電ステーションに要求するなど、電力を制御するための通信と電力の制御が行われる。

CAN バスのメッセージは容易に偽造できるため、充電用の CAN バスだけで充電制御を行うと、なりすまされた制御メッセージによって間違った電力供給が実行されることがある。しかし、CAHdeMO のようにアナログ線を組み合わせると、CAN バスへのメッセージの送信だけでは電力の制御はできない。一般的に、CAN バスへのメッセージの注入はパソコンを利用することで容易に可能だが、これにタイミングを合わせてアナログ線を制御する場合、専用のハードウェアを開発する必要があるため、やや難易度が高い。

4.2.3.2　欧米の充電制御インタフェース

欧米では Home Plug GreenPHY という電力線通信(PLC: Power Line Communication)仕様を使って充電器と自動車が通信する方式が ISO/IEC で標準化されつつある。EV と充電ステーションの間の通信路の保護は、インターネットで広く利用されている TCP 用の通信保護手順である TLS[61]を利用する[62]。この充電制御手順は IEC 15118 “Vehicle to Grid – Communication Interface” (Part 1, Part 2, Part 3)として 2012 年 1 月現在、標準化作業が進められており[63]、米国 SAE の充電制御インタフェース仕様との協調が図られている[64]。

ただし、欧米の充電制御インタフェースでは、充電時の課金やスマートグリッドとの連携など機能拡張について検討されているが、情報セキュリティについては主だった活動が見当たらない。

4.2.3.3　i-MiEV 用 CAN ゲートウェイ

「i-MiEV 用 CAN ゲートウェイ」は、三菱自動車工業の EV「i-MiEV」内部の情報のうち、充電状況などの情報を CAN プロトコルで自動車の外部に接続した機器に提供するための機器である。i-MiEV 用 CAN ゲートウェイが提供する情報は車速、駆動用バッテリー充電率、充電状況等がある。セキュリティ対策として、自動車の外部の機器から i-MiEV 内部の CAN バスへの書き込みを禁止し、さらに i-MiEV 内部の CAN 情報のうち必要なデータだけを再編成して出力することで、CAN ID 等の情報の流出を防ぐ対策している。

4.2.4　車載診断インタフェース(OBD)の接続

現在の OBD (On Board Diagnostics)は、自動車の車載制御システム内の ECU やセンサ、配線などの故障を診断、表示する機能である。自動車に故障診断機を接続して利用する(図 4-2 の E)。そのためのコネクタは OBD-II (On Board Diagnosis-II)として標準化され、自動車への搭載が義務化されている。OBD の機能の一覧を以下にまとめる。

(1)　故障診断機能: 排気ガス対策用

(2)　故障診断機能: 排ガス対策以外のエアバッグ、トランスミッション、タイヤなど

(3)　故障履歴機能

(4)　車載ソフトウェアの更新機能

---

[61] “The Transport Layer Security (TLS) Protocol Version 1.2”, IETF, 2008-08, http://tools.ietf.org/html/rfc5246
“Prohibiting Secure Sockets Layer (SSL) Version 2.0”, IETF, 2011-03, http://tools.ietf.org/html/rfc6176

[62] “ISO/IEC 国際会議出席報告書、10th Vehicle to Grid Communication Interface”、日本規格協会、2009-03-16 http://www.jsa.or.jp/itn/report2009/9146.pdf

[63] “ISO TC 22/SC 3 - Electrical and electronic equipment” http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=46752

[64] “PEV Connectivity Standards … Global Perspective”, U.S. Department of Energy, 2011-03-05 http://publicaa.ansi.org/sites/apdl/Documents/Meetings%20and%20Events/EDV%20Workshop/Presentations/Hardy-ANSI-EDV-0411.pdf

上記の機能のうち、自動車への搭載が義務化されているのは排気ガス対策用の故障診断機能だけである。その他の機能はメーカによっては搭載されていないこともあり、搭載されていたとしてもメーカごとの独自の命令や故障診断コード(DTC: Diagnostic Trouble Code)となっている。

日本では国土交通省が「J-OBD-II 活用ガイドライン[65]」で(1)と(2)の故障診断機能の利活用について普及を進めている。ISO の WWH-OBD では、「UDS (Unified Diagnostic Services)」(ISO 14229[66])で、上記の(1)から(4)のすべての機能と、TCP/IP 接続(ISO 14300: DoIP: Diagnostic communication over Internet Protocol [67])を含む CAN 以外の接続方式も OBD-II 上で利用できるよう標準化中である。

4.2.5 ITS 機能の接続

ITS の範囲は非常に幅広いが、本節では ITS 機能を ETC (Electronic Toll Collection)や ITS スポットなど路側機や車車間通信によって実現する機能として分類した(図 4-2 の F)。ETC は有料道路などでの料金収受システムを、ITS スポットは道路沿いに設置された汎用の情報提供無線通信サービスを指す。

ITS 機能の接続手法は、自動車の ITS 業界で標準化された「狭域通信」(DSRC: Dedicated Short Range Communication)がある。DSRC には日本独自の無線通信方式である ARIB T75 と TCP/IP ベースのアプリケーションインタフェース ARIB T88[68]がある。ITS Forum は 2011 年 6 月に運転支援通信システムに関する「運用管理ガイドライン」と「セキュリティガイドライン」を発行し公開している[69]。セキュリティガイドラインでは運用モデルと想定するサービスについて、システム上の脅威とリスクの分析を行っている。その上でセキュリティ対策として(1)車車間・路車間の通信メッセージの真正性と完全性、機密性の確保、(2)鍵情報漏えい時の被害拡大の最小限化、(3)交換・蓄積される資産情報は回線・機器を管理する主体が適切な保護を行う、としている。具体的なメッセージの真正性、完全性の保護方法としては、IEEE 1609.2[70]の公開鍵アルゴリズムによる電子署名方式を推奨している。

---

65 “「J - OBD II を活用した点検整備に係る情報の取扱指針」”, 国土交通省, 2011-02
http://www.mlit.go.jp/report/press/jidosha09_hh_000041.html

66 “ISO 14229: Road vehicles -- Unified diagnostic services (UDS) -- Part 1: Specification and requirements”, ISO TC22 SC3, 2009-08-14,
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45293

67 ISO 13400-1:2011 “Road vehicles -- Diagnostic communication over Internet Protocol (DoIP) -- Part 1: General information and use case definition”, ISO TC20 SC14, 2011-07-08
http://www.iso.org/iso/catalogue_detail.htm?csnumber=53765

68 “Standards for 5.8GHz DSRC”, ITS フォーラム 路側通信システム専門委員会
http://www.itsforum.gr.jp/Public/J3Schedule/P10/j2_dsrc.pdf

69 “「運転支援通信システムに関する運用管理ガイドライン」「運転支援通信システムに関するセキュリティガイドライン」の発行について”, ITS 情報通信システム推進会議, 2011-06-14,
http://www.itsforum.gr.jp/Public/J7Database/p38/P38.html

70 “ITS Standards Fact Sheets, IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE)”, USDOT RITA, http://www.standards.its.dot.gov/fact_sheet.asp?f=80

欧米では DSRC 用の無線通信方式は無線 LAN をベースにした IEEE 802.11p を、アプリケーションインタフェースは IEEE 1609 を標準化している[71]。通信を保護するためのセキュリティ仕様は IEEE 1609.2 に定義されている。IEEE 1609.2 仕様に含まれる公開鍵インフラ(PKI: Public Key Infrastructure)は自動車や組込み向けの適切な製品やサービスがなかったが、2.1.2 で紹介した PRESERVE プロジェクトで開発し、実証実験が行われる予定である。

4.2.6 テレマティクス車載機の接続

テレマティクス車載機は自動車に搭載した端末などの形で、自動車の車外との間で情報交換する装置である。テレマティクスモジュールは車載 LAN の情報を収集し、自動車のドアロックの施錠・開錠など、一部の機器の制御を行う場合もある(図 4-2 の G)。

テレマティクス車載機が使用する自動車の外部との接続方法としては、主に車載の携帯電話モジュールを利用する。また、車載の無線 LAN 機能や Bluetooth 機能を使ってガソリンスタンドや充電ステーション、家庭のアクセスポイントに接続通信する場合がある。これらの無線通信は保守用の機器との接続を容易にするためにも使われることがある。テレマティクス端末の中には音声通信をサポートし、車内のハンズフリーシステムを利用した音声通話でオペレータに問合せできる機能や、自動車事故などの緊急時でも搭乗者に代わって緊急通報を自動または半自動で行えるようにするシステムもある。

テレマティクス端末と車載 LAN とは CAN バスなどを用いて接続され、ECU の故障診断情報を収集したり、ドアロックやエアコンなど自動車の一部の制御を行う。

ここでは、北米を中心に 500 万加入者以上に普及しており、サードパーティ API を公開すると発表した OnStar の例と、テレマティクスモジュールの接続方式を紹介する。

---

[71] “IEEE Standards Association (IEEE SA) ITS Standards, 3rd ETSI TC-ITS Workshop”, IEEE 1609 WG, 2011-02-09
http://docbox.etsi.org/workshop/2011/201102_ITSWORKSHOP/08_INTERNATIONAL_ITS_STANDARDIZATION/IEEE_KURIHARA.pdf

4.2.6.1 OnStar FMV

図 4-5 ルームミラー一体型のテレマティクスモジュール- OnStar FMV 本体とリモコン

図 4-5 は General Motors 社(以下 GM)が展開する OnStar というテレマティクスサービスに対応した車載端末「FMV (For My Vehicle)」である。本体はルームミラーと一体型になっており、GM 社製の自動車なら中古車でも取り付けて使用でき、2012 年 1 月時点での取り付け可能な自動車の数は合計 9 千万台であると示されている[72]。

OnStar FMV は音声だけのガイドであればカーナビサービスにも対応しており、スマートフォンアプリを利用してドアロックなどの遠隔制御も可能である。端末価格は$199 で米国の消費者市場で手ごろな価格になっている。OnStar への加入者数は 500 万件以上と発表されている [40]。

4.2.6.2 OnStar FMV の特徴

OnStar FMV の特徴は、テレマティクスサービスとして緊急通報、盗難車追機能を提供しながら、ハンズフリーシステムにもなり、音声によるナビゲーションも含まれている点である。

OnStar ではスマートフォンに対応アプリ「RemoteLink Mobile App」を追加インストールすることで、OnStar FMV を搭載した自動車のドアロックを施錠・解除したり、エンジンスタート、ライト点滅・ホーン鳴動操作が可能である。

[72] OnStar FMV, http://www.onstar.com/web/fmv/home

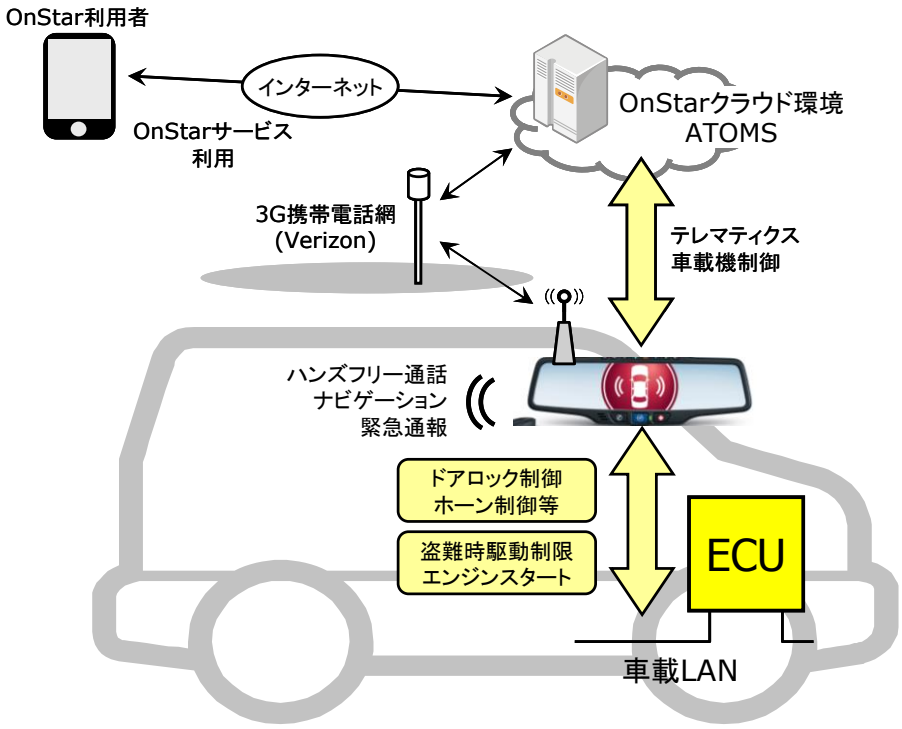

図 4-6 OnStar 用テレマティクス車載機の接続構成

図 4-6 は OnStar 用テレマティクス車載機 FMV の接続構成である。OnStar FMV 車載機は前述のようなドアロックやエンジンスタータ、ライトなど自動車の一部機能を制御するため、図の下にあるように CAN バスなどの車載 LAN にも接続している。自動車の遠隔通信については図の左上にあるスマートフォンから、クラウド環境を経由してテレマティクス車載機を制御している。

OnStar では盗難対策として、盗難車に対してエンジン回転数がアイドル回転に近くなるまでエンジン出力を下げるよう遠隔から制御する機能があり[40]、駆動系の制御に直接または間接的に制御を行っている。情報セキュリティ上の課題がセーフティに影響を与える可能性がある。

OnStar ではすでに ATOMS (Advanced Telematics Operating System)を利用して eNAV というスマートフォン向けナビ用地図サービスを提供している。ATOMS の API を利用する最初のパートナーには、RelayRides という OnStar ユーザ向けの個人間カーシェアリングサービスがある[73]。

[73] RelayRides, https://relayrides.com/

4.2.7　車載オーディオとスマートフォンの接続

ここでは車載カーナビや車載オーディオ機器(以下、車載機)と、車内に持ち込んだスマートフォンの接続方式について整理する(図 4-2 の H と I)。

従来はメディアプレーヤの操作を手動で行い、アナログ出力を車載オーディオにケーブルで入力したり、フラッシュメモリを車載オーディオに USB ケーブルで接続し、ディスクとしてマウントして利用していた。現在は、スマートフォン上のアプリで利用できるインターネットラジオで再生した音楽や、ニュースサイトでテキストを読み上げた音声を、車載オーディオで操作して再生する機能が普及しつつある。一般的にスマートフォンには USB、無線 LAN、Bluetooth などを搭載しており、車載オーディオとの接続方式はさまざまである。

共通しているのは、ハンドル周辺に装備したボタンを使って操作ができることと、映像の表示、音楽の再生などが車載のディスプレイとスピーカで行われることである。以下に、車載機とスマートフォンの接続形態について 4 つの例を示す。

(1)　MirrorLink[74]　(ターミナルモード)

スマートフォンの画面を RTP (Real-time Transport Protocol)で転送し、スマートフォン上で実行されるアプリケーションの機能を車載機の操作で利用できるようにする。通信方式は TCP/IP を利用するため接続方法は Bluetooth、無線 LAN、USB ケーブルのどれでもよい。

(2)　Bluetooth SPP (Serial Port Profile)[75]

スマートフォンを操作することで車載カーナビを操作することができる。デンソーはスマートフォン上で選択した目的地データを車載カーナビに簡単に設定するために利用している。Bluetooth の A/V (Audio Visual)制御用の機能よりも細かく車載機を制御できる特徴がある。

(3)　車載機の音声コマンドから Bluetooth 経由でスマホ上のアプリを操作

特に音声コマンドを車載機側で処理してコマンドとして認識してから、スマートフォン上のアプリを操作することができる。

(4)　Bluetooth 経由で車載機からスマートフォン上のアプリを操作

車載機などで共通的に使われている仕組みで、車載機からスマートフォンのアプリを操作する。スマートフォン側にスマートフォンを制御するための中継アプリを常駐させておく方式。

---

[74] “MirrorLink”, Car Connectivity Consortium, http://www.mirrorlink.com/

[75] “Serial Port Profile (SPP)”, Bluetooth SIG
https://www.bluetooth.org/Building/HowTechnologyWorks/ProfilesAndProtocols/SPP.htm

4.2.8　今後期待される車載 LAN の技術

2010 年度調査 [4] で SEIS (Security Embedded IP-based System)[76]の活動として車載 LAN の TCP/IP 化と情報セキュリティについて紹介した。車載 Ethernet とそれに伴う TCP/IP 化は標準化の途上にあるため将来の技術であるが、その後進展があったため報告する。市場への導入見込みの順に、図 4-2 では診断保守(E)、インフォテイメント(H)、安全快適機能(D)、駆動系(A)、シャーシ系(B)が該当する。

4.2.8.1　車載 Ethernet の標準化

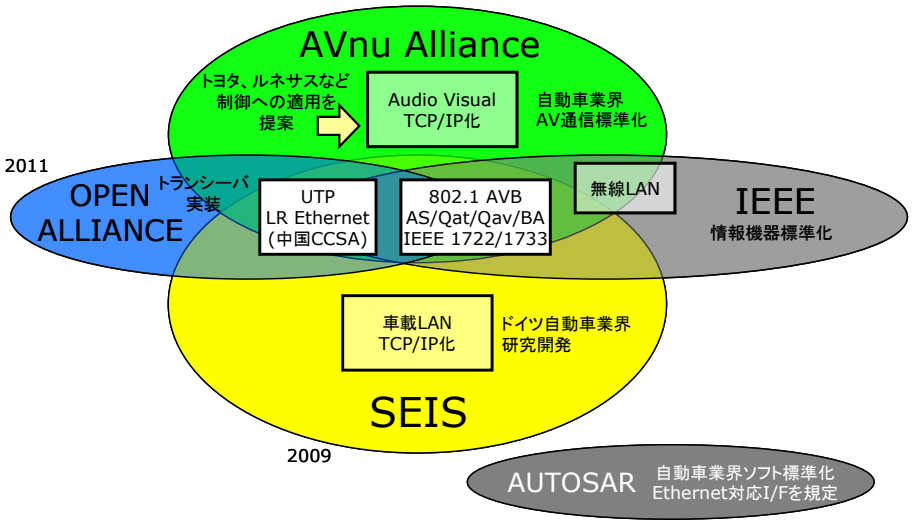

図 4-7 車載 Ethernet の主な関連団体と関係

図 4-7 は車載 Ethernet の主な関連団体と関係を示した図である。図の上、AVnu Alliance[77] は Ethernet の精密な時刻同期機能を標準化してオーディオ・ビジュアルシステムの伝送に Ethernet を利用できるようにした団体である。図の右中央、IEEE は AVnu Alliance が標準化した Ethernet AVB 仕様に含まれている時刻同期や品質制御などの詳細の標準化を行っている。OPEN ALLIANCE[78] は BroadCom を中心とする、Ethernet AVB 対応の Ethernet コントローラやスイッチ用部品を作るメーカの団体である。図下の SEIS[76] は BMW などドイツの自動車メーカを中心とした業界団体で、車載 LAN の TCP/IP 化を目指して車載 Ethernet の実用化と実証実験を行っている。図右下の AUTOSAR は車載ソフトウェアの基本制御機能を標準化する国際的な自動車業界団体だが、現在のところ直接的に車載 Ethernet の標準化に関係していないため図中では離して配置している。

---

[76] SEIS: Sicherheit in Eingebetteten IP-basierten Systemen
http://www.strategiekreis-elektromobilitaet.de/public/projekte/seis/seis-sicherheit-in-eingebetteten-ip-basierten-systemen

[77] AVnu Alliance, http://www.avnu.org/

[78] OPEN ALLIANCE SIG, http://www.opensig.org/

4.2.8.2 車載 Ethernet とその特徴

車載用としては BMW が 2008 年に車載診断インタフェース(OBD)のひとつとして Ethernet を搭載し、高速なソフトウェア書き換え(flashing)に利用している。車載用ソフトウェアは 1GB を超えることもあり、CAN の 500Kbps 通信の場合はソフトウェア書き換えのために数時間以上かかる。通信速度を Ethernet によって 100Mbps から 1Gbps 程度に高速化すると、数十秒程度でソフトウェア書き換えが済むことになり作業時間を大幅に短縮できる。

BMW では同じ 2008 年にリアシートのエンターテイメント用に従来型のシールドつき配線で Ethernet を導入している。BMW では今後 2013 年に駐車支援カメラシステムを Ethernet ベースで導入する予定である[79]。

車載 Ethernet の特徴は、銅線のケーブルにシールドが不要で芯線が 1 対で済む点である。従来の Ethernet はケーブルからの電磁放射を規制値以下に抑えるため、2 本のより対線を 2-4 組まとめたあと、さらに外側に網状のシールドで保護する必要があった。そのため一般的に Ethernet ケーブルは直径 6-8mm 以上と太く、自動車の車載配線として不適当だった。

車載 Ethernet では、配線ケーブルのシールドを不要にした 2 本のより対線(UTP: Unshielded Twisted Pair、シールドなしツイストペアケーブル)だけで 100Mbps 通信時の電磁放射の規制をクリアできるようにしている。そのため Ethernet による車載 LAN が従来の車載 LAN で使われている安価な CAN 用のツイストペアケーブルで実現できることになる。

4.2.8.3 車載 Ethernet に関する業界の動向

SEIS[76] では車載 LAN を TCP/IP 化したときの情報セキュリティについて、開発時のフレームワークの利用や、EVITA の利用を想定しているもよう[80]だが、具体的な方法は見当たらない。

AUTOSAR ではリリース 4.0 で Ethernet をサポートするための要求仕様[81]を定義している。この中では TCP/IP と DoIP のインタフェースについても触れられているが、セキュリティに関する仕様は AUTOSAR の CSM 以外には見当たらない。

車載 Ethernet を利用した製品例としては、通信機能を提供するトランシーバ製品が BroadCom 社など複数のメーカから発売または発表されている。

---

[79] “Freescale Technology Forum: Ethernet for Automotive Applications”, Dr. Robert Bruckmeier, General Manager Central Control Units, BMW Group, 2010-06
http://www.freescale.com/files/ftf_2010/Americas/WBNR_FTF10_AUT_F0558.pdf

[80] “Deliverable D1.2.5.2:Presentation Slides from the Final EVITA Workshop on Security of Automotive On-Board Networks”, EVITA Project, 2011-11-23

[81] “Requirements on Ethernet Support in AUTOSAR V1.0.0 R4.0 Rev 1”, AUTOSAR, 2009-12-07
http://www.autosar.de/download/R4.0/AUTOSAR_SRS_Ethernet.pdf

4.3　自動車のネットワーク接続の動向分析

本章におけるネットワーク接続の動向調査から、車載機を含めた自動車関連システムの「ネットワーク接続」と「オープン化」が挙げられる。自動車の付加価値を高めるため、スマートフォンやテレマティクス端末、アプリケーションなど接続が多様化し、連携動作の増加によって車載制御システムは複雑化している。また、Bluetooth や Wi-Fi などの標準的でオープンな技術の普及が順調に進みつつ、車載 Ethernet や OBD の IP 化(DoIP)など、さらにインターネットの標準的な技術を取り入れてオープン化する動向がある。また、自動車の各種センサや ECU が連携する「安全快適機能」においては、外部情報が自動車の制御にも影響を与えるようになってきている。

図 4-8 は「ネットワーク接続」、「オープン化」、「安全快適機能」の 3 つのイメージ図である。

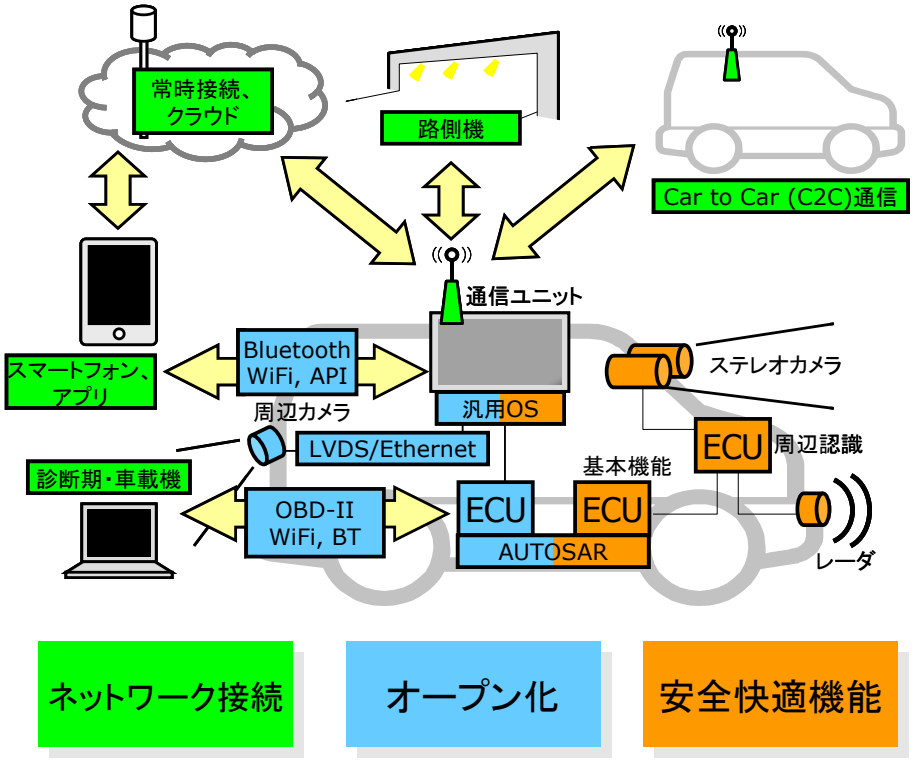

図 4-8 ネットワーク接続、オープン化、安全快適機能

ネットワーク接続は、自動車が外部の機器やサーバ、車内に持ち込んだ機器などと多様な手段で相互接続し連携する状況を示している。「オープン化」は自動車に搭載される機器や技術が標準化され、容易に接続・制御しやすくなっている状況を示している。「安全快適機能」は、セーフティや快適性のために追加された機能が自動車の制御システムに影響を及ぼしていることを示す。

4.3.1.1　ネットワーク接続の多様化・複雑化による影響

自動車のネットワーク接続にインターネット等で利用されている標準規格の利用が進むことで、様々な車内外の機器や情報システムが繋がっていくことが考えられる。これによって、自動車の利用者が様々なサービスを利用することが可能になる一方で、自動車の制御情報やユーザの個人情報など、自動車を利用する上で守るべき情報資産も拡大していく。また、本章で紹介したスマートフォン上のアプリと車載機の連携 API の実行環境については、他のスマートフォンのアプリや他のサイトの不具合による攻撃被害の可能性も考えられ、車載制御システムだけでは対応できない問題も含まれる。

それと同時に車載制御システムは多様な接続によって、情報セキュリティ上の問題が影響する範囲が拡大している。従来は車載 LAN への直接の接続はないと考えられていたカーナビも、グローバル市場に対応するために CAN バスへの接続することがある。テレマティクス端末については特に自動車メーカが提供するサービスではドアロックの制御のほか、エンジン出力の低減、ソフトウェアの更新サービスなどを提供するものがあり、自動車の基本的な制御機能への影響力を増している。将来は車載 Ethernet や故障診断の TCP/IP 対応(DoIP)などにより、侵入経路の数と容易さが格段に増す。

上記のように、標準的な技術を利用した多様な接続により情報セキュリティの被害を受けやすい状況で、同時に自動車の基本的な制御機能への影響を及ぼさないために、被害が影響を及ぼす範囲を限定するしくみが必要である。

4.3.1.2　車載システムのオープン化における影響

車載システムや車内外のネットワークがオープン化される事で、これまで情報システムで発生していたものと同様の脅威を、自動車についても検討する必要がある。ただし、現状では OBD-II や CAN 通信での認証機能が個別のメーカごとに実装されている現状であり、暫くの間は標準技術と個別技術が混在する中で、セキュリティ対策を模索することになると考えられる。

その一方、UDS など故障診断機能や車載 Ethernet、PLC による TCP/IP 対応の充電制御インタフェースの国際標準化については、情報セキュリティへの対応方法に関する公開情報が一部のみであったため、今後の標準化動向の確認または標準化への参加・寄与が必要である。

将来的には OBD によって試験の自動化も国際的に標準化された場合、攻撃者にとっては脆弱性のスキャンが容易になる問題があるが、情報セキュリティ対策者は「OVAL (Open Vulnerability and Assessment Language)[82]」や「SCAP (Security Content Automation Protocol)[83]」のような IT 業界で普及しつつあるセキュリティの自動診断手順を自動車の情

[82] “セキュリティ検査言語 OVAL 概説”, IPA, 2011-09-28, http://www.ipa.go.jp/security/vuln/OVAL.html
[83] “セキュリティ設定共通化手順 SCAP 概説”, IPA, 2010-06-24, http://www.ipa.go.jp/security/vuln/SCAP.html

報システムでも利用できる可能性があり、実現すれば自動車の情報セキュリティ対策を大幅に効率化できる。また、今後のコスト競争や汎用的なサービスの普及が展開されていく中で、CAN や LIN など自動車特有の通信手順から、車載 Ethernet や TCP/IP など共通化された通信手順に移行する事が考えられるため、EVITA 等の既存の自動車関連セキュリティ対策に関しても、それに併せた活動が行われることが予測される。

4.3.1.3 安全快適機能の拡大とネットワーク接続からの影響

現在、急速に機能追加が行われている安全快適機能に対して、本節で整理したネットワーク接続が徐々に連携を始めている。カーナビはナビアシストによる運転支援機能が安全快適機能と関連し、周辺カメラによる障害物や交通標識などの認識結果は駐車支援や急発進防止、注意喚起などの安全運転支援に関連している。そして ITS 機能は将来的に出会い頭衝突の回避や前方の危険回避を自動化する情報源として期待されている。

現在のところ安全快適機能に直接関与するネットワーク接続はほとんどないが、将来的に安全快適機能がネットワーク接続からの情報をもとに車載 LAN を経由して「走る・曲がる・止まる」を制御することが期待されている現在、安全快適機能がネットワーク接続から受ける影響について情報セキュリティの面からも検討や整理を行う必要がある。

なお、ネットワーク接続の問題は単なる入り口の問題である場合もある。例えば安全快適機能はその多くの部分がソフトウェアで実現されているため、実行されるソフトウェアが正しいソフトウェアと設定であることを検証できれば、セキュリティ上の深刻な被害を避けられることもある。こうした主要な問題を特定する作業は 2010 年度版報告書にあるように、セキュリティ上の脅威をツリー状に分析することで対応できる。

5　まとめ

本調査のまとめとして、自動車情報セキュリティに関する現状と課題を整理する。

5.1　進化する自動車と増大する脅威

4.3 節で示した「ネットワーク接続」「オープン化」「安全快適機能」の３つの要素は自動車の進化、価値の向上をもたらす反面、人命に影響を与える重大な脅威をもたらす可能性がある。また、3 章で整理したように自動車情報セキュリティの脆弱性は年々着実に増大しており、それに対して 2 章で整理したように国内外での情報セキュリティ対策はこれからという状況である。

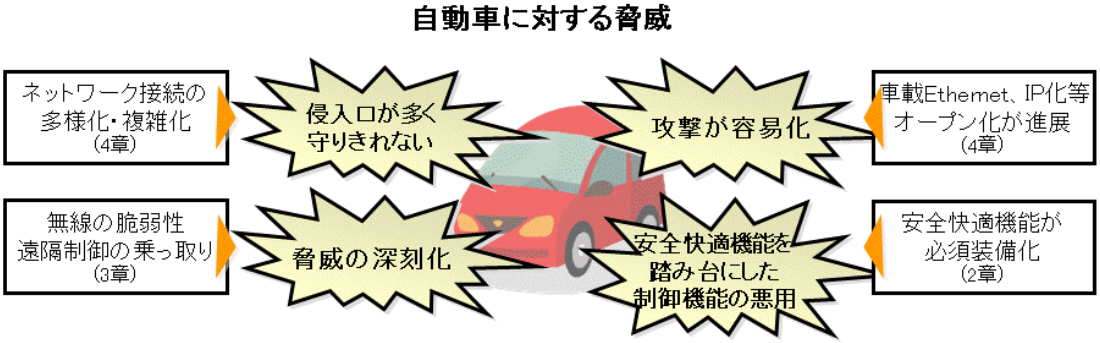

図 5-1 自動車に対する脅威

このような状況においては、オープンな技術の脆弱性を突いた攻撃やネットワーク経由での攻撃、安全快適機能において車両制御を行うシステムを利用した制御系への攻撃などにより、重大な被害がもたらされる可能性がある。

図 5-2 は、研究会及びディスカッショングループで検討した自動車への情報セキュリティ上の脅威を取りまとめたものである。図中の黄色枠は脅威の例、矢印は脅威の流れを示している。本図から以下のことが分かる。

(1)　自動車の様々な機能が外部通信手段を持つ事によって、車載システムを含めた自動車関連機器に対して様々な脅威が存在する

(2)　自動車の駆動系やシャーシ系に対して直接セキュリティ上の脅威が発生することは考えにくいが、車載システムを踏み台にした間接的な攻撃が行われる可能性がある

これらの課題について、次節で整理する。

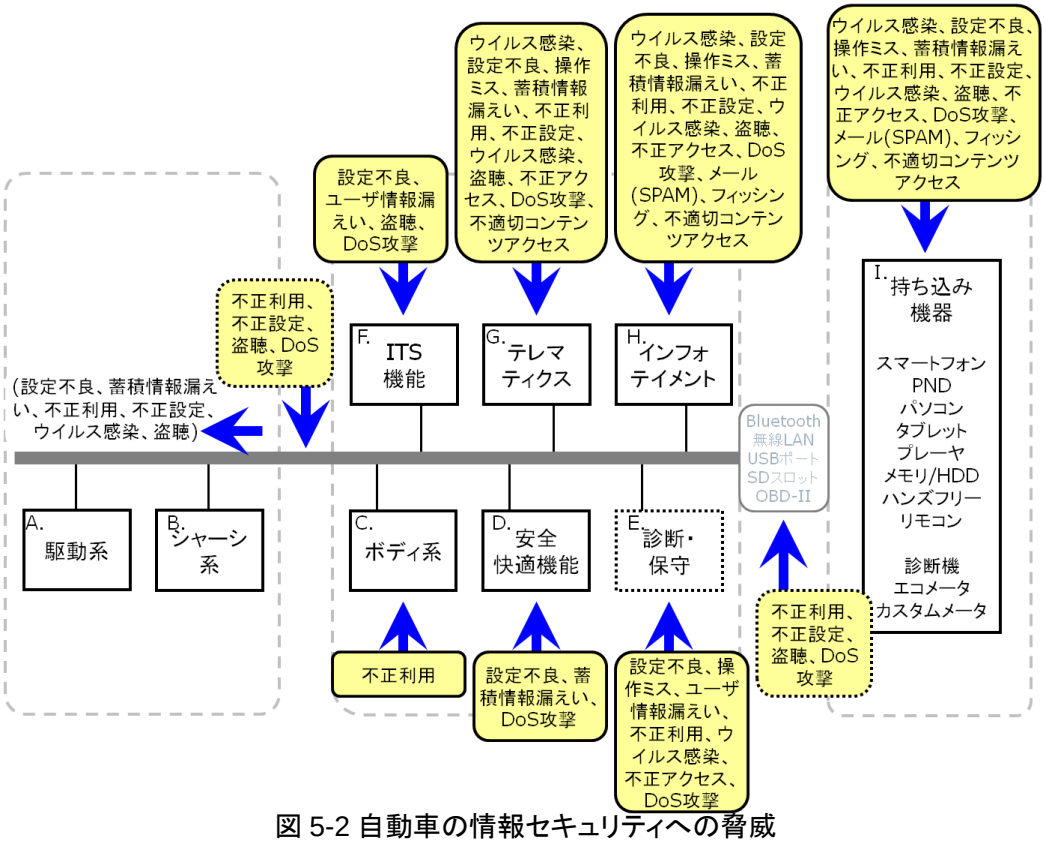

図 5-2 自動車の情報セキュリティへの脅威

5.2 自動車情報セキュリティの課題

現状のまとめから、自動車情報セキュリティの課題を整理する。

5.2.1 スマートフォンなど「ネットワーク接続」を経由した攻撃の拡大

4 章で説明したとおり、「ネットワーク接続」を活用した安全快適機能やプローブ情報・CAN バスの情報の活用などにより、自動車の機能は高まっている。また、エンターテイメント機能の充実や電気自動車の蓄電池の活用など、「走る・止まる・曲がる」という基本制御機能を超えた新たな価値を持ちつつある。特にスマートフォンは、ユーザが車内に持ち込み、様々な自動車用のアプリを活用したり、車載機とインターネット等の外部ネットワークを繋ぐ仲介をさせることで、利便性や快適性を向上させるための重要な機器となりつつある。

しかしながら、自動車が様々な通信を行う事によって、その通信を悪用した攻撃が発生する事が考えられる。特に、スマートフォン等を通して自動車とインターネットが常時接続されるようになると、現在の情報システムで発生しているような脅威に対するセキュリティ対策が必要となってくる。

5.2.2 「オープン化」による攻撃容易性の増大

車載制御システムではこれまで、自動車独自の CAN バスや LIN バスなどが採用されている。また車載制御システム上で交換されるメッセージやデータの形式はメーカや車種ごとに独自であり、故障応答コードや故障診断機の互換性がなかった。

しかし、4 章で示したとおり、車載制御システムの基幹である車載 LAN と診断保守インタフェースである OBD に TCP/IP を利用した仕組みの標準化が進められている。また、すでに OBD-II ポートや CAN バスを無線通信に変換するアダプタは複数販売されており、一部メーカでは標準装備化している。一方で、アプリケーション実行環境も自動車業界の AUTOSAR 標準や、スマートフォンやタブレットの Android、iOS のような業界標準 OS が車載機でも採用され始めている。

利便性やコスト削減の追求から、これまでそれぞれの自動車メーカが独自で開発・利用していた車載システムに、情報システムにおいて既に標準化された技術が採用されたり、自動車メーカ間で新たにデータフォーマット等の標準化が進むことで、自動車全体の「オープン化」は今後も進んでいくことが考えられる。標準化された技術は、独自技術等よりはその仕様や仕組みが一般に公開されることが多くなる上、攻撃者による解析にさらされる可能性も高くなるため、攻撃の容易性が増大する可能性がある。

5.2.3 「安全快適機能」を利用した自動車の基本制御機能への攻撃可能性

2 章で示したとおり、近年の自動車にはセンサなどからの情報を基に、「走る・曲がる・止まる」といった基本制御機能をサポートする安全快適機能が普及しつつある。センサや通信機器を通して自動車外部から情報を取得することでユーザの安全や快適な運転を実現する取組みは、操作ミスやわき見運転等のヒューマンエラー防止や、自動車同士が連携することによるサービスの向上等、安全性・利便性の向上が期待される。

しかしながら、ネットワーク接続を利用した悪意のある攻撃により「走る・曲がる・止まる」機能が設計時には想定外の動作をさせられると、エンジンやブレーキ、ステアリングなどが期待どおりに制御されず、人命に関わる重大な被害が生じる可能性がある。

6　自動車情報セキュリティへの提言

ここでは自動車情報セキュリティについて、これまでの動向と課題に対する提言を行う。自動車情報セキュリティへの提言は図 6-1 にあるように 3 つである。

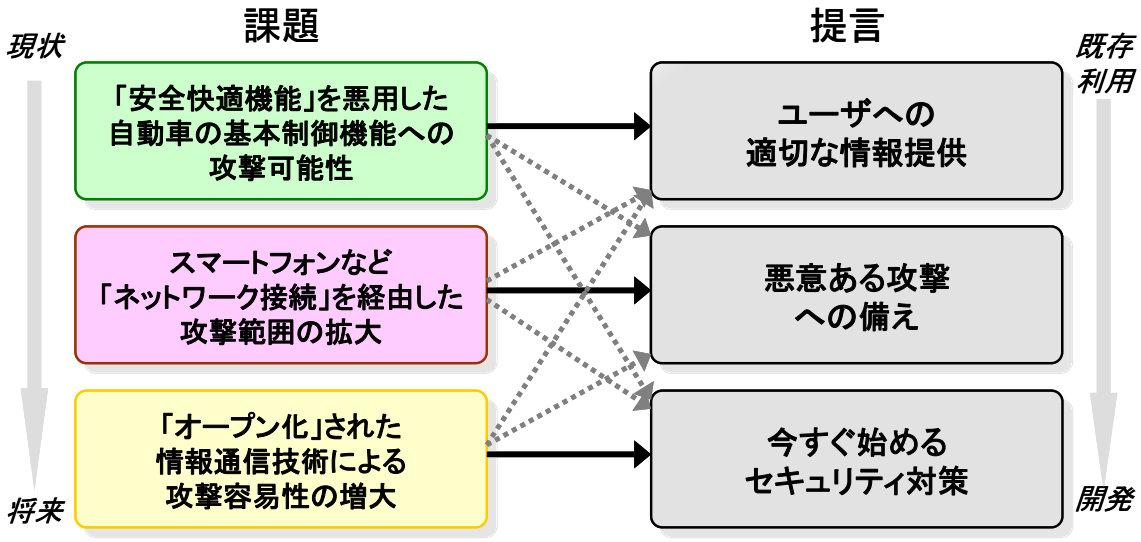

図 6-1 自動車情報セキュリティへの提言

6.1　ユーザへの適切な情報提供

6.1.1　接続手法、資産情報の整理及び脅威の想定

スマートフォンなどネットワーク接続による脅威を想定するために、自動車及び周辺機器の開発者は自動車のネットワーク接続手法及びそこで利用される資産情報を洗い出し、整理する必要がある。

情報資産については、カーナビの内部に蓄積･格納された住所や電話番号等の個人情報、起点/終点を含む経路案内履歴、ドライブレコーダの記録などのほか、ECU やカーナビ、テレマティクス車載機内のセキュリティなどについて洗い出し、重要度やリアルタイムで守る必要性などについて整理する必要がある。

また、スマートフォンやカーナビ、テレマティクス車載機などの機器を利用したネットワーク経由でのサービス内容のほか、常時接続やソフトウェア書換え、機器制御の有無などについて把握し、サービスや機器が停止した場合の影響や、利用者が注意すべき点について整理する必要がある。

6.1.2　適切な利用･管理方法の周知

前述の、ネットワーク接続手法や情報資産についての整理結果に基づいてユーザが知るべき情報セキュリティに関する事項を取りまとめ、様々な手段でユーザに周知していくことが必要である。

本調査は自動車の開発者を主な対象にしているが、カーパーツショップや整備工場などアフタ市場で車載機を取り付ける事業者、自動車向けにサービスを提供する事業者にも、ユーザに自動車の情報セキュリティに関する事項の周知が求められる。

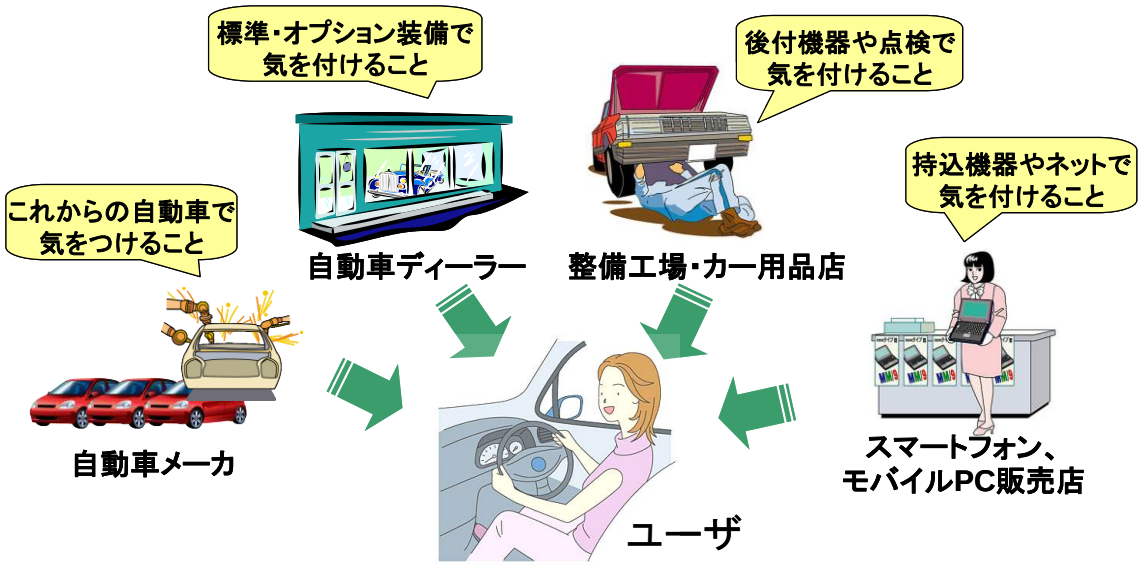

図 6-2 ユーザへの適切な情報提供

重要事項は取扱説明書にも記載されると想定されるが、現状では取扱説明書の冒頭にある重要な注意事項は 100 件にも上る。自動車の利用者に見ていただくためには、スマートフォンやタブレットなど、持ち込み機器を活用した周知方法も検討が必要である。

6.1.3　新しい用途の把握と対応

4 章の調査結果にあるように、スマートフォンやテレマティクスによる自動車向けサービスは日々進化しており、サービス内容も多様化するとともに、プライバシに関する情報を扱うなど、リスクがあるものも多い。今後新しい機器やサービスが発達していくに従って、それに応じた情報資産や脅威が発生することが考えられる。そのため、新しい機器やサービスについて、適宜、サーベイを行い、リスクを把握するとともに、ユーザに周知していくことが必要である。

6.2　悪意ある攻撃への備え

6.2.1　セーフティとセキュリティの両立

自動車のセーフティについては、「機能安全」を実現するための国際標準規格が ISO/DIS 26262 として策定され、基本的な設計手順や基準が整えられている。しかし、3 章で示したように、自動車が様々な通信手法を持ち、それを活用した技術が発達する中では、現在の自動車は故障や過失だけでなく、悪意のある攻撃者からの攻撃への対応が必要である。

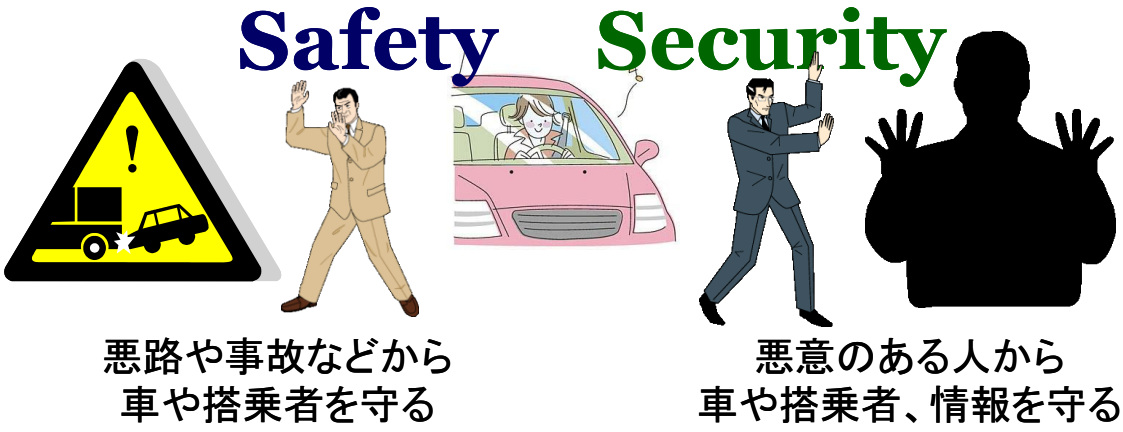

図 6-3 悪意ある攻撃の認識

4 章で紹介したような多数のネットワーク接続手法において、情報セキュリティ対策はメーカやサービスごとに個別に行われており、対策が行われていないものもある。セーフティ同様、情報セキュリティに対しても適切かつ十分な対策が必要である。

6.2.2　自動車が攻撃対象となる認識の必要性

情報通信技術の進展により自動車の情報化も急速に進展しており、さまざまな機能やサービスが追加され、自動車には「走る・曲がる・止まる」に留まらない価値が生まれている。これによって、自動車は今までの盗難や車上荒らしといった直接的な攻撃だけではなく、情報漏洩や盗聴等の情報システム上の攻撃にさらされる可能性も高まってきている。実際に、情報セキュリティ研究者の間では、自動車の情報制御システムに対する攻撃の動機の高まりによって、自動車が「次のハッキングの開拓地」になると予測されている[84]。

数年以内には実用化されると見られる自動運転機能や自動ブレーキの普及や、日米欧で導入が進む ITS 等のための車車間通信や大規模な遠隔制御などについて、それを対象とした攻撃や対策について、事前にしっかりと検討することが重要となる。

---

[84] “Cars: The next hacking frontier?”, CNET, 2010-08-31, http://news.cnet.com/8301-27080_3-20015184-245.html

6.3　今すぐ始めるセキュリティ対策

大規模化・分散化しつつある車載制御システムにおいて、抜けの無い情報セキュリティ対策を実施することは簡単ではない。また、深刻なリスクを緩和しないまま製品を市場に送り出した結果、脅威が顕在化した後にセキュリティ対策を実施すると非常に大きなコストがかかる。そのため、自動車の情報セキュリティにおいて先行している欧州の研究開発事例や、生産設備などを対象とした制御システムセキュリティの対策、家電やスマートフォン等の組込みセキュリティの対策を参考に、自動車の情報セキュリティについても、今から検討を始める必要がある。

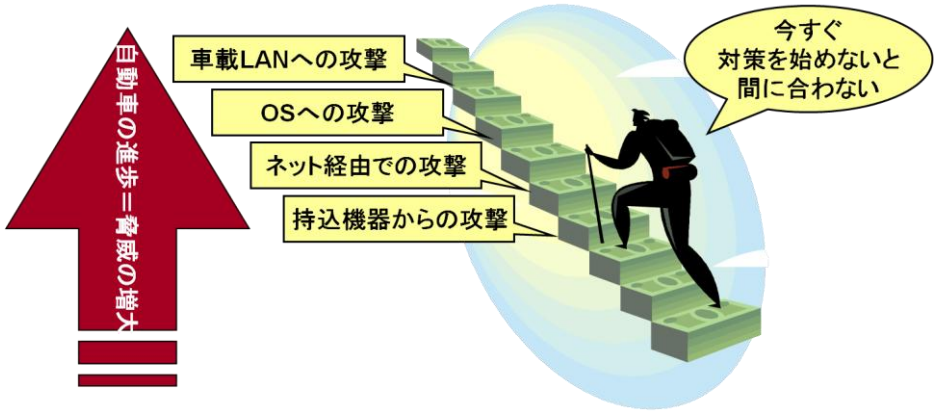

図 6-4 今すぐはじめるセキュリティ対策

6.3.1　オープン化による攻撃の容易化への対応

4 章で示したように、車載 LAN が段階的に Ethernet 化されたり、OBD-II の TCP/IP 化が実現すれば、車載情報システムへの攻撃は飛躍的に容易になっていくと考えられる。これは、HTML5 など汎用的な Web の標準技術をカーナビなどの車載機に利用する場合も同様である。

標準的な技術を利用することで、製品は実装方式や通信方式などに自動車特有のプロトコル等が大幅に減るため、攻撃者は攻撃が容易になる。製品の側では従来のような自動車の独自技術による実装上の制約が減り、製品の外部にあった障壁がほぼなくなるため、製品の内部に攻撃を防ぐか、攻撃が成立しないようなしくみを取り入れる必要がある。そのため例えば通信メッセージの暗号化や通信先の ECU などの認証を行うことがあるが、こうしたセキュリティ機能の実装は機能の検証や相互運用性の確保の点で難易度が高い。セキュリティ機能を利用する場合はできるだけフレームワークなどの開発支援環境の上でカプセル化された機能を利用するなど、開発プロセスに簡単に取り入れる必要がある。

6.3.2　オープン技術とネットワーク接続の活用

自動車におけるオープン化とネットワーク接続は、攻撃の糸口となることで脅威をもたらす面があるが、適切に利用することでソフトウェアの実行環境を安全に保つことができる面もある。例えば、オープンな技術が繰り返し利用される事によって、その技術を利用する上でのセキュリティ上の懸念点が洗い出され、技術として洗練される事が期待される他、汎用的なセキュリティ対策を導入する事が可能となる。また、ネットワーク接続によって車載ソフトウェアを適切に更新することで、既に出荷されて運用段階にある自動車に対して、車載制御システムの不具合や脆弱性を解消し、情報セキュリティを保つことができる。

一方で、ネットワーク接続によって車載制御システムへの情報セキュリティの侵害情報や脆弱性の情報を収集することで、正確な攻撃の実態を把握することができる。また攻撃に対してはネットワーク接続を通じて対策や情報提供を行うことにより、被害が及ぶ範囲を限定することができる。

6.3.3　他組織の情報セキュリティ対策との連携

自動車の情報セキュリティは対象範囲が従来から広い。車載制御システムの開発組織を基本としているが、スマートフォン等の後付けのデバイスや自動車の情報を利用したサービスベンダなど、自動車を利用する上では多数の組織がその開発・運用に関わっており、規模が大きい。また、車室内での音声・ビジュアル・その他情報処理、持ち込み機器の接続と連携、移動しながらの無線通信、クラウドやスマートグリッドとの協調など他の分野への広がりもある。一方、情報セキュリティの分野においては、攻撃する側もアンダーグラウンド市場で組織として分業体制が構成されている場合もあり、攻撃手法も日に日に洗練されていく傾向にある。

このような広い範囲かつ強力な敵に対して自動車業界だけで情報セキュリティの対応を実施することは難しい。それぞれに対応する業界組織や標準化団体と連携して、自動車の情報セキュリティ対策を実現する必要がある。そのために自社内に限らず、自動車に関連する他組織の情報セキュリティ対策の情報交換と、協調した行動が必要である。